

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-085048

(43)Date of publication of application : 20.03.2003

(51)Int.Cl.

G06F 12/14  
G06F 12/00  
G06F 12/16  
G09C 1/00  
H04L 9/08  
H04L 9/32

(21)Application number : 2001-274746

(71)Applicant : SONY CORP

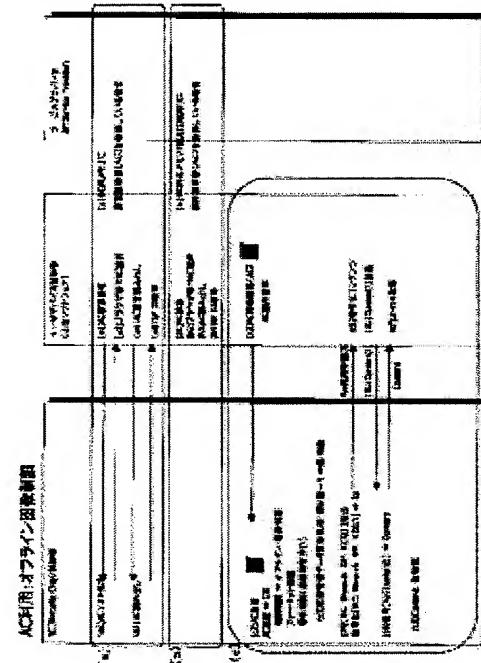
(22)Date of filing : 11.09.2001

(72)Inventor : SHIMADA NOBORU  
ISHIBASHI YOSHITO  
ABE HIROSHI  
OKA MAKOTO

## (54) BACKUP DATA MANAGEMENT SYSTEM, BACKUP DATA MANAGEMENT METHOD, AND INFORMATION PROCESSING DEVICE, AND COMPUTER PROGRAM

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a system capable of executing backup data management in an information processing device securely and efficiently.  
**SOLUTION:** Backup object data are enciphered by a backup key, and enciphered key data acquired by enciphering the backup key by using a public key of a support center which is an external entity are generated, and the generated data are stored in media or transmitted to the support center. In restore processing of the backup data, a partitioned region is set in a memory in the information processing device following an attribute certificate for memory region security, and the data are stored. Hereby, there is no possibility of being decoded even if a backup data storage medium is transferred to a third party, to thereby reduce the load of the backup data management in a user device, and to facilitate management under high grade security of the data.



(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-85048

(P2003-85048A)

(43)公開日 平成15年3月20日(2003.3.20)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テマコト <sup>8</sup> (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
12/00	5 3 1	12/00	5 3 1 M 5 B 0 1 8
12/16	3 1 0	12/16	3 1 0 M 5 B 0 8 2
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B 5 J 1 0 4
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 B

審査請求 未請求 請求項の数15 OL (全 82 頁) 最終頁に続く

(21)出願番号 特願2001-274746(P2001-274746)

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(22)出願日 平成13年9月11日(2001.9.11)

(72)発明者 島田 昇

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72)発明者 石橋 義人

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74)代理人 100101801

弁理士 山田 英治 (外2名)

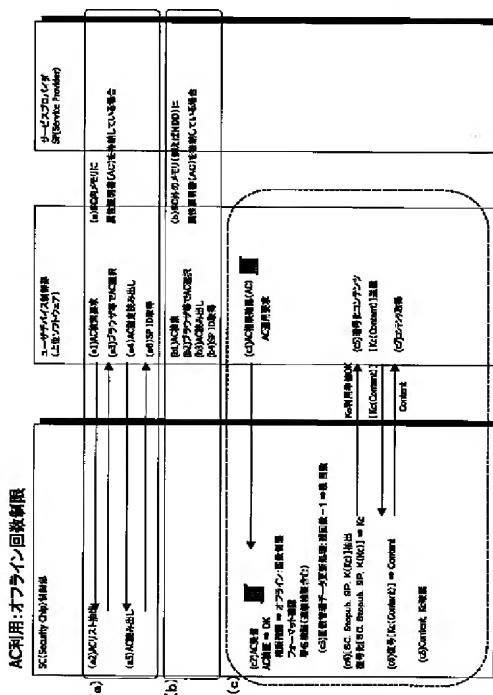
最終頁に続く

(54)【発明の名称】 バックアップデータ管理システム、バックアップデータ管理方法、および情報処理装置、並びにコンピュータ・プログラム

(57)【要約】

【課題】 情報処理装置におけるバックアップデータ管理をセキュアにかつ効率的に実行可能としたシステムを実現する。

【解決手段】 バックアップ対象データをバックアップ鍵で暗号化するとともに、バックアップ鍵を外部エンティティであるサポートセンタの公開鍵を用いて暗号化した暗号化鍵データを生成し、生成データをメディアに格納、またはサポートセンタに送信する。バックアップデータのリストア処理は、メモリ領域確保用属性証明書に従って情報処理装置のメモリに区分領域を設定し、格納する。第三者にバックアップデータ格納メディアが渡ったとしても復号される恐れがなく、ユーザデバイスにおけるバックアップデータ管理の負担が軽減され、データの高度なセキュリティの下での管理が容易となる。



## 【特許請求の範囲】

【請求項1】情報処理装置におけるバックアップデータの管理を実行するバックアップデータ管理システムであり、

前記情報処理装置は、

バックアップ対象データをバックアップ鍵で暗号化した暗号化バックアップデータと、前記バックアップ鍵を外部エンティティであるサポートセンタの公開鍵を用いて暗号化した暗号化鍵データとを生成し、生成データをバックアップ用メディアに格納、またはサポートセンタに送信する構成を有し、

前記サポートセンタは、該サポートセンタの秘密鍵を適用した前記暗号化鍵データの復号化処理により、バックアップ鍵を取得し、取得したバックアップ鍵を適用した暗号化バックアップデータの復号によりバックアップデータを取得し、前記取得したバックアップデータを情報処理装置に格納する処理を実行する構成を有することを特徴とするバックアップデータ管理システム。

【請求項2】前記情報処理装置は、

前記バックアップ鍵を、前記バックアップメディアに対するデータ格納時に使用する一時的な鍵として生成し、バックアップ処理後に、該バックアップ鍵を前記情報処理装置内のメモリに格納することなく消去する処理を実行する構成を有することを特徴とする請求項1に記載のバックアップデータ管理システム。

【請求項3】前記サポートセンタは、

バックアップデータの転送元であるサポートセンタサーバと、バックアップデータの転送先である情報処理装置との間の相互認証の成立を条件として、バックアップデータの情報処理装置への格納処理を実行する構成であることを特徴とする請求項1に記載のバックアップデータ管理システム。

【請求項4】前記バックアップ対象データは、

前記情報処理装置のメモリ内に設定される区分領域に格納されるデータであり、

前記情報処理装置は、メモリ領域確保用属性証明書に記録された領域確保条件に従って、前記メモリ内に区分領域を設定する処理を実行する構成を有し、

前記サポートセンタは、メモリ領域確保用属性証明書と、バックアップデータとを前記情報処理装置に対して出力し、

前記情報処理装置は、

前記メモリ領域確保用属性証明書に従って前記情報処理装置内のメモリに区分領域を設定し、該設定した区分領域に前記バックアップデータを格納する処理を実行する構成を有することを特徴とする請求項1に記載のバックアップデータ管理システム。

【請求項5】前記情報処理装置は、

メモリ領域確保用属性証明書に従って前記情報処理装置内のメモリに区分領域を設定し、該設定した区分領域に

前記バックアップデータを格納する処理を実行する構成を有し、

前記情報処理装置は、

前記メモリ領域確保用属性証明書の署名検証処理を実行し、該署名検証によりメモリ領域確保用属性証明書の正当性が確認されたことを条件として、前記情報処理装置内のメモリに区分領域を設定する処理を実行する構成であることを特徴とする請求項1に記載のバックアップデータ管理システム。

【請求項6】情報処理装置におけるバックアップデータの管理を実行するバックアップデータ管理方法であり、前記情報処理装置において、

バックアップ対象データをバックアップ鍵で暗号化した暗号化バックアップデータと、前記バックアップ鍵を外部エンティティであるサポートセンタの公開鍵を用いて暗号化した暗号化鍵データとを生成し、生成データをバックアップ用メディアに格納、またはサポートセンタに送信し、

前記サポートセンタにおいて、

該サポートセンタの秘密鍵を適用した前記暗号化鍵データの復号化処理により、バックアップ鍵を取得し、取得したバックアップ鍵を適用した暗号化バックアップデータの復号によりバックアップデータを取得し、前記取得したバックアップデータを情報処理装置に格納する処理を実行することを特徴とするバックアップデータ管理方法。

【請求項7】前記情報処理装置は、

前記バックアップ鍵を、前記バックアップメディアに対するデータ格納時に使用する一時的な鍵として生成し、

バックアップ処理後に、該バックアップ鍵を前記情報処理装置内のメモリに格納することなく消去する処理を実行することを特徴とする請求項6に記載のバックアップデータ管理方法。

【請求項8】前記サポートセンタは、

バックアップデータの転送元であるサポートセンタサーバと、バックアップデータの転送先である情報処理装置との間の相互認証の成立を条件として、バックアップデータの情報処理装置への格納処理を実行することを特徴とする請求項6に記載のバックアップデータ管理方法。

【請求項9】前記バックアップ対象データは、前記情報処理装置のメモリ内に設定される区分領域に格納されるデータであり、

前記サポートセンタは、メモリ領域確保用属性証明書と、バックアップデータとを前記情報処理装置に対して出力し、

前記情報処理装置は、

前記メモリ領域確保用属性証明書に従って前記情報処理装置内のメモリに区分領域を設定し、該設定した区分領域に前記バックアップデータを格納する処理を実行することを特徴とする請求項6に記載のバックアップデータ

管理方法。

【請求項10】前記情報処理装置は、メモリ領域確保用属性証明書の署名検証処理を実行し、該署名検証によりメモリ領域確保用属性証明書の正当性が確認されたことを条件として、前記情報処理装置内のメモリに区分領域を設定する処理を実行することを特徴とする請求項6に記載のバックアップデータ管理方法。

【請求項11】データ処理を実行する情報処理装置であり、

バックアップ対象データをバックアップ鍵で暗号化した暗号化バックアップデータと、前記バックアップ鍵を外部エンティティであるサポートセンタの公開鍵を用いて暗号化した暗号化鍵データとを生成し、生成データをバックアップ用メディアに格納、またはサポートセンタに送信する構成を有することを特徴とする情報処理装置。

【請求項12】前記情報処理装置は、前記バックアップ鍵を、前記バックアップメディアに対するデータ格納時に使用する一時的な鍵として生成し、バックアップ処理後に、該バックアップ鍵を前記情報処理装置内のメモリに格納することなく消去する処理を実行する構成を有することを特徴とする請求項11に記載の情報処理装置。

【請求項13】前記バックアップ対象データは、前記情報処理装置のメモリ内に設定される区分領域に格納されるデータであり、

前記情報処理装置は、メモリ領域確保用属性証明書に従って前記情報処理装置内のメモリに区分領域を設定し、該設定した区分領域に前記バックアップデータを格納する処理を実行する構成を有することを特徴とする請求項11に記載の情報処理装置。

【請求項14】前記情報処理装置は、メモリ領域確保用属性証明書の署名検証処理を実行し、該署名検証によりメモリ領域確保用属性証明書の正当性が確認されたことを条件として、前記情報処理装置内のメモリに区分領域を設定する処理を実行する構成であることを特徴とする請求項11に記載の情報処理装置。

【請求項15】情報処理装置におけるバックアップデータの管理を実行するバックアップデータ管理処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、

バックアップ対象データをバックアップ鍵で暗号化した暗号化バックアップデータを生成するステップと、前記バックアップ鍵を外部エンティティであるサポートセンタの公開鍵を用いて暗号化した暗号化鍵データを生成するステップと、

を有することを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、バックアップデー

タ管理システム、バックアップデータ管理方法、および情報処理装置、並びにコンピュータ・プログラムに関する。特に、情報処理装置におけるデータ処理の開始条件として設定されるパスワードの管理を、セキュアにかつ効率的に実行することを可能としたバックアップデータ管理システム、バックアップデータ管理方法、および情報処理装置、並びにコンピュータ・プログラムに関する。

【0002】

【従来の技術】昨今、音楽データ、画像データ、ゲームプログラム等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）を、インターネット、衛星を介した通信他、有線、無線の各種通信網を介して配信するサービスが盛んになってきている。また、DVD、CD、メモリカード等の流通可能な記憶媒体を介したコンテンツ流通も盛んになってきている。これらの流通コンテンツは、ユーザの所有する例えば、TV、PC（Personal Computer）、再生専用器、あるいはゲーム機器等において、再生、利用される。

【0003】通信網を介して配信されるコンテンツは、例えば通信機能を有するセットトップボックスによって受信され、TV他の再生装置において再生可能なデータに変換されて再生されたり、あるいは通信インターフェースを備えたTV、再生装置、ゲーム機器、PC等の情報機器によって受信されて再生される。

【0004】ゲームプログラム、音楽データ、画像データ等、多くのソフトウェア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウェアの使用を許諾し、許可のない複製等が行われないようにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。

【0005】ユーザに対する利用制限を実現する1つの手法が、配布コンテンツの暗号化処理である。例えば著作権保護の要請されるコンテンツを衛星通信あるいはインターネット通信等を介した配信、あるいはDVD等のメディアに格納して配布する場合にコンテンツを暗号化して配信または格納し、正規ユーザに対してのみコンテンツ復号に利用可能な復号鍵を配布する。正規ユーザは配布された復号鍵によって暗号化コンテンツの復号を実行し、コンテンツを再生する構成である。

【0006】暗号化データは、復号鍵を用いた復号化処理によって復号データ（平文）に戻すことができる。データ暗号化処理に暗号化鍵を用い、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。

【0007】暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類あるが、その1つの例としていわゆる共通鍵暗号化方式と呼ばれている方式

がある。共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式にDES(データ暗号標準:Data encryption standard)がある。

【0008】上述の暗号化処理、復号化に用いられる暗号化鍵、復号化鍵は、例えばあるパスワード等に基づいてハッシュ関数等の一方向性関数を適用して得ることができる。一方向性関数とは、その出力から逆に入力を求めるのは非常に困難となる関数である。例えばユーザが決めたパスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵、復号化鍵を生成するものである。このようにして得られた暗号化鍵、復号化鍵から、逆にそのオリジナルのデータであるパスワードを求めることは実質上不可能となる。

【0009】また、暗号化するときに使用する暗号化鍵による処理と、復号するときに使用する復号化鍵の処理とを異なる鍵で行なう方式がいわゆる公開鍵暗号方式と呼ばれる方式である。公開鍵暗号方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が生成した公開鍵を用いて暗号化処理を行なう。公開鍵によって暗号化された文書は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号化処理が可能となる。秘密鍵は、公開鍵を生成した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号することができる。公開鍵暗号方式の代表的なものには、楕円曲線暗号、あるいはRSA(Rivest-Shamir-Adleman)暗号がある。このような暗号化方式を利用することにより、暗号化コンテンツを正規ユーザに対してのみ復号可能とするシステムが可能となる。

#### 【0010】

【発明が解決しようとする課題】上記のようなコンテンツ利用管理システムでは、コンテンツを暗号化してユーザにネットワーク、あるいはDVD、CD等の記録媒体に格納して提供し、暗号化コンテンツを復号するコンテンツ鍵を正当なユーザにのみ提供する構成が多く採用されている。コンテンツ鍵自体の不正な利用等を防ぐためのコンテンツ鍵を暗号化して正当なユーザに提供し、正当なユーザのみが有する復号キーを用いて暗号化コンテンツ鍵を復号してコンテンツ鍵を使用可能とする構成が提案されている。

【0011】正当なユーザであるか否かの判定は、一般には、例えばコンテンツの送信者であるコンテンツプロバイダとユーザデバイス間ににおいて、コンテンツ、あるいはコンテンツ鍵の配信前に認証処理を実行することによって行なう。一般的な認証処理においては、相手の確認を行なうとともに、その通信でのみ有効なセッション

キーを生成して、認証が成立した場合に、生成したセッションキーを用いてデータ、例えばコンテンツあるいはコンテンツ鍵を暗号化して通信を行なう。

【0012】例えば上述の認証処理に必要な鍵データ、ユーザデバイスIDなどのデータは第三者に漏洩することのないように管理することが必要となる。従って、このような秘密データは第三者によるアクセスがなされないよう、パスワード等によってアクセス権を確認することが行なわれる。

【0013】しかし、このような秘密情報は、例えばユーザデバイスの故障等によりアクセスが不能となる場合に備えて何らかのメディアにバックアップデータとして格納しておくことが必要となる場合がある。ただし、バックアップデータに基づくデータ漏洩を考慮した場合、暗号化処理を行なった上でバックアップを行なうことが好ましいが、デバイスから取り出せる鍵を用いた暗号化処理を行なうと、不正な第三者によって鍵が取得され、機密データが復号されて漏洩する可能性がある。

【0014】本発明は、上述の問題点に鑑みてなされたものであり、バックアップデータの管理におけるユーザの負担を軽減し、バックアップデータの漏洩防止を図り、さらに、バックアップデータに基づくリストア処理も効率的にかつセキュアに実行することを可能としたバックアップデータ管理システム、バックアップデータ管理方法、および情報処理装置、並びにコンピュータ・プログラムを提供することを目的とする。

#### 【0015】

【課題を解決するための手段】本発明の第1の側面は、情報処理装置におけるバックアップデータの管理を実行するバックアップデータ管理システムであり、前記情報処理装置は、バックアップ対象データをバックアップ鍵で暗号化した暗号化バックアップデータと、前記バックアップ鍵を外部エンティティであるサポートセンタの公開鍵を用いて暗号化した暗号化鍵データとを生成し、生成データをバックアップ用メディアに格納、またはサポートセンタに送信する構成を有し、前記サポートセンタは、該サポートセンタの秘密鍵を適用した前記暗号化鍵データの復号化処理により、バックアップ鍵を取得し、取得したバックアップ鍵を適用した暗号化バックアップデータの復号によりバックアップデータを取得し、前記取得したバックアップデータを情報処理装置に格納する処理を実行する構成を有することを特徴とするバックアップデータ管理システムにある。

【0016】さらに、本発明のバックアップデータ管理システムの一実施態様において、前記情報処理装置は、前記バックアップ鍵を、前記バックアップメディアに対するデータ格納時に使用する一時的な鍵として生成し、バックアップ処理後に、該バックアップ鍵を前記情報処理装置内のメモリに格納することなく消去する処理を実行する構成を有することを特徴とする。

【0017】さらに、本発明のバックアップデータ管理システムの一実施態様において、前記サポートセンタは、バックアップデータの転送元であるサポートセンタサーバと、バックアップデータの転送先である情報処理装置との間の相互認証の成立を条件として、バックアップデータの情報処理装置への格納処理を実行する構成であることを特徴とする。

【0018】さらに、本発明のバックアップデータ管理システムの一実施態様において、前記バックアップ対象データは、前記情報処理装置のメモリ内に設定される区分領域に格納されるデータであり、前記情報処理装置は、メモリ領域確保用属性証明書に記録された領域確保条件に従って、前記メモリ内に区分領域を設定する処理を実行する構成を有し、前記サポートセンタは、メモリ領域確保用属性証明書と、バックアップデータとを前記情報処理装置に対して出力し、前記情報処理装置は、前記メモリ領域確保用属性証明書に従って前記情報処理装置内のメモリに区分領域を設定し、該設定した区分領域に前記バックアップデータを格納する処理を実行する構成を有することを特徴とする。

【0019】さらに、本発明のバックアップデータ管理システムの一実施態様において、前記情報処理装置は、メモリ領域確保用属性証明書に従って前記情報処理装置内のメモリに区分領域を設定し、該設定した区分領域に前記バックアップデータを格納する処理を実行する構成を有し、前記情報処理装置は、前記メモリ領域確保用属性証明書の署名検証処理を実行し、該署名検証によりメモリ領域確保用属性証明書の正当性が確認されたことを条件として、前記情報処理装置内のメモリに区分領域を設定する処理を実行する構成であることを特徴とする。

【0020】さらに、本発明の第2の側面は、情報処理装置におけるバックアップデータの管理を実行するバックアップデータ管理方法であり、前記情報処理装置において、バックアップ対象データをバックアップ鍵で暗号化した暗号化バックアップデータと、前記バックアップ鍵を外部エンティティであるサポートセンタの公開鍵を用いて暗号化した暗号化鍵データとを生成し、生成データをバックアップ用メディアに格納、またはサポートセンタに送信し、前記サポートセンタにおいて、該サポートセンタの秘密鍵を適用した前記暗号化鍵データの復号化処理により、バックアップ鍵を取得し、取得したバックアップ鍵を適用した暗号化バックアップデータの復号によりバックアップデータを取得し、前記取得したバックアップデータを情報処理装置に格納する処理を実行することを特徴とするバックアップデータ管理方法にある。

【0021】さらに、本発明のバックアップデータ管理方法の一実施態様において、前記情報処理装置は、前記バックアップ鍵を、前記バックアップメディアに対するデータ格納時に使用する一時的な鍵として生成し、バッ

クアップ処理後に、該バックアップ鍵を前記情報処理装置内のメモリに格納することなく消去する処理を実行することを特徴とする。

【0022】さらに、本発明のバックアップデータ管理方法の一実施態様において、前記サポートセンタは、バックアップデータの転送元であるサポートセンタサーバと、バックアップデータの転送先である情報処理装置との間の相互認証の成立を条件として、バックアップデータの情報処理装置への格納処理を実行することを特徴とする。

【0023】さらに、本発明のバックアップデータ管理方法の一実施態様において、前記バックアップ対象データは、前記情報処理装置のメモリ内に設定される区分領域に格納されるデータであり、前記サポートセンタは、メモリ領域確保用属性証明書と、バックアップデータとを前記情報処理装置に対して出力し、前記情報処理装置は、前記メモリ領域確保用属性証明書に従って前記情報処理装置内のメモリに区分領域を設定し、該設定した区分領域に前記バックアップデータを格納する処理を実行することを特徴とする。

【0024】さらに、本発明のバックアップデータ管理方法の一実施態様において、前記情報処理装置は、メモリ領域確保用属性証明書の署名検証処理を実行し、該署名検証によりメモリ領域確保用属性証明書の正当性が確認されたことを条件として、前記情報処理装置内のメモリに区分領域を設定する処理を実行することを特徴とする。

【0025】さらに、本発明の第3の側面は、データ処理を実行する情報処理装置であり、バックアップ対象データをバックアップ鍵で暗号化した暗号化バックアップデータと、前記バックアップ鍵を外部エンティティであるサポートセンタの公開鍵を用いて暗号化した暗号化鍵データとを生成し、生成データをバックアップ用メディアに格納、またはサポートセンタに送信する構成を有することを特徴とする情報処理装置にある。

【0026】さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、前記バックアップ鍵を、前記バックアップメディアに対するデータ格納時に使用する一時的な鍵として生成し、バックアップ処理後に、該バックアップ鍵を前記情報処理装置内のメモリに格納することなく消去する処理を実行する構成を有することを特徴とする。

【0027】さらに、本発明の情報処理装置の一実施態様において、前記バックアップ対象データは、前記情報処理装置のメモリ内に設定される区分領域に格納されるデータであり、前記情報処理装置は、メモリ領域確保用属性証明書に従って前記情報処理装置内のメモリに区分領域を設定し、該設定した区分領域に前記バックアップデータを格納する処理を実行する構成を有することを特徴とする。

【0028】さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、メモリ領域確保用属性証明書の署名検証処理を実行し、該署名検証によりメモリ領域確保用属性証明書の正当性が確認されたことを条件として、前記情報処理装置内のメモリに区分領域を設定する処理を実行することを特徴とする。

【0029】さらに、本発明の第4の側面は、情報処理装置におけるバックアップデータの管理を実行するバックアップデータ管理処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、バックアップ対象データをバックアップ鍵で暗号化した暗号化バックアップデータを生成するステップと、前記バックアップ鍵を外部エンティティであるサポートセンタの公開鍵を用いて暗号化した暗号化鍵データを生成するステップと、を有することを特徴とするコンピュータ・プログラムにある。

【0030】なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能なコンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【0031】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

### 【0032】

【発明の実施の形態】【システム概要】図1に本発明のコンテンツ利用管理システムにおける各エンティティ、および各エンティティの処理の概要を説明する図を示す。

【0033】ユーザデバイス101は、コンテンツを利用する各ユーザの端末であり、具体的には、PC、ゲーム端末、DVD、CD等の再生装置、記録再生装置等である。これらの端末には、後段で説明する暗号処理、コンテンツ利用処理を制御する制御手段を備えた耐タンパ構成のセキュリティチップが装着されている。コンテンツ配信エンティティ（コンテンツディストリビュータ）としてのサービスプロバイダ（SP-CD）102、その他のエンティティとユーザデバイス101間で実行されるデータ転送等におけるユーザデバイス101側のセキュアな処理の多くは、セキュリティチップ内で制御、実行される。

【0034】サービスプロバイダ（コンテンツディストリビュータ）（SP-CD）102は、セキュリティチ

ップを持つユーザデバイス101に対してコンテンツを提供するサービスプロバイダである。コンテンツクリエータ103は、サービスプロバイダ（コンテンツディストリビュータ）（SP-CD）102に対してサービスに供するためのコンテンツを提供する。ユーザデバイス製造者（Manufacturer）104は、ユーザデバイス101を製造するエンティティである。

【0035】サポートセンタ105は、ユーザデバイス101に装着されたユーザデバイスでの様々な処理に対するサポートを実行するセンタであり、例えばユーザが認証情報として利用するパスワードを忘れた場合のパスワードのリカバリ処理、あるいはユーザデバイスが生成したコンテンツのバックアップデータを利用したリストア（復旧）処理など、ユーザデバイスに対する様々なサポート処理を実行する。認証局（CA：Certification Authority）106は各エンティティに対して公開鍵証明書（PKC：Public Key Certificate）を発行する。

【0036】なお、ユーザデバイス101、サービスプロバイダ（コンテンツディストリビュータ）（SP-CD）102、コンテンツクリエータ103、ユーザデバイス製造者（Manufacturer）104、サポートセンタ105、認証局（CA：Certification Authority）106、各エンティティの数は任意である。特に、図1において、認証局（CA：Certification Authority）106を1つのみ示してあるが、認証局は、各エンティティでの処理に応じて必要となる公開鍵証明書を発行する複数の認証局が存在してよい。

【0037】ユーザデバイス101は、衛星通信、インターネット通信、あるいはその他、有線、無線のデータ通信ネットワークを介してサービスプロバイダ（コンテンツディストリビュータ）102から暗号化されたコンテンツを受信し、コンテンツを利用する。暗号化コンテンツを復号するための鍵：コンテンツ鍵：Kcは暗号化されてコンテンツ利用権限を示す権限情報証明書としてのコンテンツ利用権限証明書、例えば属性証明書（AC：Attribute Certificate）110に格納されており、ユーザ端末101がコンテンツを復号して利用するためには、サービスプロバイダ（コンテンツディストリビュータ）102から属性証明書（AC：Attribute Certificate）110を受領し、セキュリティチップを持つユーザデバイスにおいて属性証明書から鍵を取り出して復号することが必要となる。

【0038】コンテンツ利用権限を示す権限情報証明書としてのコンテンツ利用権限証明書、例えば属性証明書（AC：Attribute Certificate）110には、暗号化されたコンテンツ鍵：Kcの他に、コンテンツの利用制限回数や利用期限など、コンテンツの利用制限情報が記録されており、ユーザデバイス101は、コンテンツ利用権限証明書としての属性証明書（AC）110に記録されたコンテンツ利用制限に従ったコンテンツの利用が

可能となる。

【0039】なお、以下、実施例の説明では、属性証明書（A C : Attribute Certificate）110にコンテンツの利用情報、暗号化コンテンツ鍵を格納した構成として説明するが、コンテンツの利用情報、暗号化コンテンツ鍵を格納した証明書は、いわゆる規定に従った属性証明書（A C）に限らず、任意のデータフォーマットの証明書として構成可能である。すなわちコンテンツの利用権限を証明するデータを格納し、データ改竄検証のための発行エンティティの署名データが付加された構成であれば、任意のデータ形式のコンテンツ利用権限証明書が利用可能である。

【0040】なお、サービスプロバイダからユーザデバイスに対するコンテンツ配信あるいは属性証明書（A C : Attribute Certificate）の配信形態としては、ユーザ側からサービスプロバイダに対する要求に基づいて実行される形態と、ユーザの要求の有無に関係なく例えばサブスクライバ契約を結んでいるユーザに対して、サービスプロバイダから一方的に送信するいわゆるプッシュ型の形態（プッシュ型モデル）のいずれの形態も可能である。

【0041】図1で示す各エンティティ中、認証局106以外のエンティティ、すなわちユーザデバイス101、サービスプロバイダ（コンテンツディストリビュータ）（S P - C D）102、コンテンツクリエータ103、およびユーザデバイス製造者（Manufacturer）104、サポートセンタ105のエンティティは、所定のルールに従ってコンテンツ利用、コンテンツ配信を可能とするため、各エンティティでの処理を所定のルールに従って実行する。このルールを設定し、管理するエンティティとして図示しないシステムホルダ（S H : System Holder）がある。図1の101～105の各エンティティは、システムホルダ（S H）の設定したコンテンツ利用インフラ、ルールの下で各エンティティでの処理を実行する。

【0042】例えばユーザデバイス製造者（Manufacturer）104は、製造するユーザデバイス内の耐タンパ構成を持つセキュリティチップ内に、コンテンツ配信において適用するデバイス識別子（I D）、および各種の暗号処理鍵を格納する。ユーザデバイス101、サービスプロバイダ（コンテンツディストリビュータ）102、コンテンツクリエータ（C C）103、サポートセンタ105間でのコンテンツ転送、属性証明書の転送、その他のデータ転送処理においては、システムホルダ（S H）の設定したルールに基づいて、例えば相互認証処理、データ暗号化処理を実行する。

【0043】また、ユーザデバイス101におけるコンテンツ利用に際しては、属性証明書に記録された利用制限を遵守したコンテンツ利用を実行する。例えば回数制限の設定されたコンテンツの利用に際してデバイス内の

セキュリティチップの制御部の制御の下に、コンテンツ利用可能回数を係数するカウンタを更新する処理等を実行する。このような各エンティティでの処理のルールを規定したプラットホームを構築し、管理するエンティティがシステムホルダ（S H）である。

【0044】【公開鍵証明書、属性証明書】図1の構成において利用される公開鍵証明書、属性証明書について、その概要を説明する。

【0045】（公開鍵証明書（P K C））公開鍵証明書について図2、図3、図4を用いて説明する。公開鍵証明書は、認証局（C A : Certification Authority）が発行する証明書であり、ユーザ、各エンティティが自己のI D、公開鍵等を認証局に提出することにより、認証局側が認証局のI Dや有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。

【0046】公開鍵証明書のフォーマット例を図2～図4に示す。これは、公開鍵証明書フォーマット I T U - T X . 5 0 9 に準拠した例である。

【0047】バージョン（version）は、証明書フォーマットのバージョンを示す。シリアルナンバー（Serial N umber）は、公開鍵証明書発行局（C A）によって設定される公開鍵証明書のシリアルナンバーである。シグネチャ（Signature）は、証明書の署名アルゴリズムである。なお、署名アルゴリズムとしては、楕円曲線暗号およびR S Aがあり、楕円曲線暗号が適用されている場合はパラメータおよび鍵長が記録され、R S Aが適用されている場合には鍵長が記録される。発行者（issuer）は、公開鍵証明書の発行者、すなわち公開鍵証明書発行局（I A）の名称が識別可能な形式（Distinguished Na me）で記録されるフィールドである。有効期限(validit y)は、証明書の有効期限である開始日時、終了日時が記録される。サブジェクト公開鍵情報(subject Public Ke y Info)は、証明書所有者の公開鍵情報として鍵のアルゴリズム、鍵が格納される。

【0048】証明局鍵識別子（authority Key Identifier、authority Cert Issuer、authority Cert Serial Number）は、署名検証に用いる証明書発行者の鍵を識別する情報であり、鍵識別子、機関証明書発行者の名称、機関証明書シリアル番号を格納する。サブジェクト鍵識別子（subject key Identifier）は、複数の鍵を公開鍵証明書において証明する場合に各鍵を識別するための識別子を格納する。鍵使用目的（key us age）は、鍵の使用目的を指定するフィールドであり、（0）ディジタル署名用、（1）否認防止用、（2）鍵の暗号化用、（3）メッセージの暗号化用、（4）共通鍵配達用、（5）認証の署名確認用、（6）失効リストの署名確認用の各使用目的が設定される。秘密鍵有効期限(private Key Usage Period)は、証明書に格納した公開鍵に対応する秘密鍵の有効期限を記録する。認証局ボ

リシー (certificate Policies) は、公開鍵証明書発行者の証明書発行ポリシーを記録する。例えば ISO/I EC 9384-1に準拠したポリシー ID、認証基準である。ポリシー・マッピング (policy Mapping) は、認証バス中のポリシー関係の制限に関する情報を格納するフィールドであり、認証局 (CA) 証明書にのみ必要となる。サブジェクト別名 (subject Alt Name) は、証明書所有者の別名を記録するフィールドである。発行者別名 (issuer Alt Name) は、証明書発行者の別名を記録するフィールドである。サブジェクト・ディレクトリ・アトリビュート (subject Directory Attribute) は、証明書所有者のために必要とされるディレクトリの属性を記録するフィールドである。基本制約 (basic Constraint) は、証明対象の公開鍵が認証局 (CA) の署名用か、証明書所有者のものかを区別するためのフィールドである。許容サブツリー制約名 (name Constraints permitted Subtrees) は、発行者が発行する証明書の名前の制限情報を格納するフィールドである。制約ポリシー (policy Constraints) は、認証バス中のポリシーの関係の制限情報を格納するフィールドである。CRL参照ポイント (Certificate Revocation List Distribution Points) は、証明書所有者が証明書を利用する際に、証明書が失効していないか、どうかを確認するための失効リストの参照ポイントを記述するフィールドである。署名アルゴリズム (Signature Algorithm) は、証明書の署名付けに用いるアルゴリズムを格納するフィールドである。署名は、公開鍵証明書発行者の署名フィールドである。電子署名は、証明書全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して発行者の秘密鍵を用いて生成したデータである。署名付けやハッシュをとるだけでは改竄は可能であるが、検出できれば実質的に改竄できないことと同様の効果がある。

【0049】認証局は、図2～図4に示す公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための失効リスト (Revocation List) の作成、管理、配布 (これをリボケーション: Revocationと呼ぶ) を行う。また、必要に応じて公開鍵・秘密鍵の生成も行う。

【0050】一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。

【0051】(属性証明書 (AC)) 属性証明書について図5を用いて説明する。属性証明書には大きく分けて2つの種類があり、1つは、コンテンツの利用権といった権利や権限に関する所有者の属性情報を含む証明書で

ある。もう1つは、サービスプロバイダ (SP) 用領域確保または削除用属性証明書 (AC) であり、ユーザデバイス内のメモリにサービスプロバイダ (SP) 用情報格納領域を確保または削除する場合の領域確保または削除の許諾情報を含む属性証明書 (AC) である。

【0052】属性証明書フォーマットはITU-T X.509で規定されており、IETF PKIX WGでProfileを策定している。公開鍵証明書とは異なり所有者の公開鍵を含まない。しかし属性証明書認証局(Attribute Certificate Authority)の署名がついているため、改竄されていないかどうかの判定はこの署名を検証することで行える、という点は公開鍵証明書と同様である。

【0053】本発明の構成においては、属性証明書 (AC) の発行管理を行なう属性証明書認証局(Attribute Certificate Authority)は、サービスプロバイダ (コンテンツディストリビュータ) (SP-CD) 102が兼務することが可能である。別の構成としてもよい。属性証明書は常に公開鍵証明書と関連づけて利用する。すなわち所有者の本人性自体は公開鍵証明書で確認し、その上で所有者にいかなる権限が与えられているかのみを示すものが属性証明書である。属性証明書の検証にあたっては、当該証明書の署名検証を行った後、それに関連づけられている公開鍵証明書の検証も行う。

【0054】なお、その際、原則的には証明書連鎖をたどって最上位の公開鍵証明書まで順に検証を実施することが好ましい。複数の認証局 (CA) が存在し、階層構成をなす認証局構成では、下位の認証局自身の公開鍵証明書は、その公開鍵証明書を発行する上位認証局によって署名されている。すなわち、下層の公開鍵証明書発行局 (CA-Low) に対して上位の公開鍵証明書発行局 (CA-High) が公開鍵証明書を発行するという連鎖的な公開鍵証明書発行構成をとる。公開鍵証明書の連鎖検証とは、下位から上位へ証明書連鎖をたどって最上位の公開鍵証明書までの連鎖情報を取得して、最上位 (ルートCA) までの公開鍵証明書の署名検証を行なうことを意味する。

【0055】属性証明書の有効期間を短期間とすることにより、失効処理を行わないことも可能である。この場合、証明書の失効手続きや失効情報の参照手順等を省くことができ、システムが簡易となる長所がある。ただし証明書の不正利用に対しては失効以外の何らかの対策が必要となるため、十分に注意しなければならない。本認証システムにおいては、コンテンツに対する利用権限の他に、コンテンツを復号するためのコンテンツ鍵を属性証明書に埋め込んでおく構成であるので、正当なコンテンツ利用権限のあるユーザデバイスは、正当な属性証明書を受領することにより、コンテンツを利用可能である。

【0056】図5に示す属性証明書の構成について説明する。証明書のバージョン番号は、証明書フォーマット

のバージョンを示す。AC保持者の公開鍵証明書情報、これは属性証明書(AC)の発行者に対応する公開鍵証明書(PKC)に関する情報であり、PKC発行者名、PKCシリアル番号、PKC発行者固有識別子等の情報であり、対応公開鍵証明書を関連づけるリンクデータとしての機能を持つ。属性証明書の発行者の名前は、属性証明書の発行者、すなわち属性証明書認証局(AA)の名称が識別可能な形式(Distinguished Name)で記録されるフィールドである。署名アルゴリズム識別子は、属性証明書の署名アルゴリズム識別子を記録するフィールドである。証明書の有効期限は、証明書の有効期限である開始日時、終了日時が記録される。属性情報フィールドは、属性証明書の利用形態に応じて、(1)メモリ領域確保、削除情報、または、(2)コンテンツ利用条件関連情報のいずれかが格納される。コンテンツ利用条件関連情報には、暗号化されたコンテンツ鍵を含む。

【0057】(1)メモリ領域確保、削除情報は、サービスプロバイダがユーザデバイスのセキュリティチップ内のメモリにサービスプロバイダ毎の管理領域を登録設定、または削除処理を目的として発行される属性証明書に記録される。記録情報は、例えば以下の情報である。

サービスプロバイダ識別子(ID)

サービスプロバイダ・ネーム

処理：メモリ領域確保、メモリ領域削除のいずれか

領域サイズ：メモリ領域のサイズ

【0058】サービスプロバイダは、上記各項目を属性情報フィールドに格納した属性証明書をユーザデバイスに対して送付し、ユーザデバイスは属性証明書の検証の後、自己のセキュリティチップ内のメモリに、受信した属性証明書の属性情報フィールドの記録に従ったメモリ領域の確保処理、または確保済みのメモリ領域の削除処理を実行する。

【0059】(2)コンテンツ利用条件関連情報は、サービスプロバイダの提供するコンテンツに対応して発行される属性証明書の属性情報フィールドに格納する情報であり、コンテンツの利用制限回数、利用期限等の様々な利用条件を含み、さらにコンテンツを暗号化したコンテンツ鍵の暗号化データを含む。記録情報は、例えば以下の情報である。

サービスプロバイダ識別子(ID)

サービスプロバイダ・ネーム

アプリケーション識別子(ID)：コンテンツの識別情報である。

条件：オンライン利用コンテンツか、オフライン利用コンテンツか、さらに、買い切りコンテンツ、期間制限コンテンツ、オンライン回数制限コンテンツ、オフライン回数制限コンテンツのいずれであるかを示す情報である。

有効期限：期間制限の場合の有効期限情報

利用制限回数：回数制限の場合の利用可能回数

支払条件：コンテンツの対価の支払条件を記録  
コンテンツ鍵：暗号化されたコンテンツ鍵を暗号化アルゴリズム情報とともに格納

【0060】コンテンツの利用態様には、上記条件フィールドに記載のように、(1)オンライン利用か、(2)オフライン利用かの区別と、(a)コンテンツを買い切りし、買い切り以後のコンテンツ利用をフリーとする態様、(b)期間制限を設けてコンテンツの利用期間を設定した態様、(c)回数制限を設けてコンテンツの利用回数を制限した態様の各態様がある。また期間制限と回数制限の両制限を伴うコンビネーション制限態様もある。ユーザデバイスでは、属性証明書に記録されたこれらの態様に従ってコンテンツの利用が実行される。これらの具体的な処理態様については、後段で説明する。

【0061】また、暗号化コンテンツの復号鍵として適用するコンテンツ鍵：Kcを暗号化した暗号化コンテンツ鍵が格納される。コンテンツ鍵：Kcの暗号化処理に直接あるいは間接的に適用する鍵の主な種類は以下に示す通りである。

(a)ユーザデバイスのセキュリティチップの各サービスプロバイダ管理領域に格納されたSP対応ストレージ秘密鍵に対応するサービスプロバイダ(SP)対応ストレージ公開鍵：SC. Stopub. SP. K、(公開鍵方式)

(b)ユーザデバイスのセキュリティチップの各サービスプロバイダ管理領域に格納されたSP対応ストレージ鍵(共通鍵方式)

(c)サービスプロバイダの保有する秘密鍵：SP. St o. K

(d)システムホルダ(SH)とユーザデバイスで共有する鍵として生成されるグローバル共通鍵：Kg  
これらの鍵を適用した処理については後段で詳細に説明する。

【0062】属性証明書には、さらに、署名アルゴリズムが記録され、属性証明書発行者である属性証明書認証局(AA)によって署名が施される。電子署名は、属性証明書全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して属性証明書発行者(AA)の秘密鍵を用いて生成したデータである。

【0063】[セキュリティチップ構成] 次にコンテンツを利用する情報処理装置としてのユーザデバイス内に構成されるセキュリティチップの構成について、図6を参照しながら説明する。なお、ユーザデバイスは、データ処理手段としてのCPU、通信機能を備えたPC、ゲーム端末、DVD、CD等の再生装置、記録再生装置等によって構成されるものであり、これらのユーザデバイスの中に耐タンパ構造を持つセキュリティチップが実装されることになる。ユーザデバイス自体の構成例は本明細書の末尾において説明する。セキュリティチップを持

つユーザデバイスは、図1におけるユーザデバイス製造者104において製造される。

【0064】図6に示すように、ユーザデバイス200には、セキュリティチップ210が、ユーザデバイス側制御部221に対して、相互にデータ転送可能な構成として内蔵される。セキュリティチップ210は、プログラム実行機能、演算処理機能を持つCPU(Central Processing Unit)201を有し、データ通信用のインターフェース機能を持つ通信インターフェース202、CPU201によって実行される各種プログラム、例えば暗号処理プログラム、デバイスの製造時に格納されるマスター鍵: Kmなどを記憶するROM(Read Only Memory)203、実行プログラムのロード領域、また、各プログラム処理におけるワーク領域として機能するRAM(Random Access Memory)204、外部機器との認証処理、電子署名の生成、検証処理、格納データの暗号化、復号化処理等の暗号処理を実行する暗号処理部205、前述したサービスプロバイダ毎の情報、各種鍵データを含むデバイスの固有情報を格納した例えばEEPROM(Electrically Erasable Programmable ROM)によって構成されるメモリ部206を有する。これら格納情報の詳細については後述する。

【0065】ユーザデバイス200は、暗号化コンテンツ等を格納する領域としてのEEPROM、ハードディスク等によって構成される外部メモリ部222を有する。外部メモリ部222は、公開鍵証明書、属性証明書の格納領域としても利用可能であり、また後段で説明するコンテンツの利用回数管理ファイルの格納領域としても利用される。

【0066】セキュリティチップを搭載したユーザデバイスが、外部エンティティ、例えばサービスプロバイダと接続し、データ転送処理を実行する場合には、必要に応じて、セキュリティチップ210と、外部エンティティ間の相互認証が行われ、また転送データの暗号化が行なわれる。これらの処理の詳細については、後段で詳述する。

【0067】ユーザデバイスのセキュリティチップでの処理対象となるデータ例を図7に示す。これらの多くは、不揮発性メモリーの一種であるフラッシュメモリ等のEEPROM(Electrically Erasable Programmable ROM)によって構成されるメモリ部206に格納されるが、製造時に格納し、書き換え不可能とするデータ、例えばマスター鍵: Kmは、ROM(Read Only Memory)203に格納される。公開鍵証明書、属性証明書は、セキュリティチップ内のメモリに格納しても、外部メモリに格納してもよい。

【0068】各データについて説明する。

公開鍵証明書(PKC)：公開鍵証明書は、第三者に対して正当な公開鍵であることを示す証明書で、証明書には配布したい公開鍵を含み、信頼のおける認証局により

デジタル署名されている。ユーザデバイスには、前述した階層構成の最上位認証局(ルートCA)の公開鍵証明書、ユーザデバイスに登録されたサービスプロバイダ、すなわち、ユーザデバイス内にメモリ領域が確保されているサービスプロバイダの公開鍵証明書、さらに、パスワード復帰処理等のサポートを実行するサポートセンタの公開鍵証明書を格納する。

【0069】属性証明書(AC)：公開鍵証明書が証明書利用者(所有者)の“本人性”を示すのに対し、属性証明書は証明書利用者の利用権限を示すものである。利用者は属性証明書を提示することにより、属性証明書に記載された権利・権限に基づいて、アプリケーションの利用や、領域の確保などが行えるようになる。以下に、属性証明書の種類を示し、それぞれの果たす役割を示す。

【0070】(a) アプリケーション利用管理用属性証明書(AC)：アプリケーションとは、一般に言われるコンテンツを広い意味で使用した表現であり、アプリケーションの種類としては、ゲーム、音楽、映画、金融情報等の各種アプリケーションがある。アプリケーション利用管理用属性証明書(AC)では、アプリケーションの利用権限に関しての記述があり、属性証明書(AC)をサービスプロバイダ(SP)に対して提示して検証、もしくは、ローカルで検証することにより、属性証明書(AC)に記述された利用権限範囲内でのアプリケーションの利用許諾が得られる。アプリケーションの利用権限に関する記述としては、アプリケーションのオンライン利用が可能であるかオフライン利用が可能であるか、さらに、オンライン利用可能なコンテンツの場合には、利用期間制限、利用回数制限情報があり、オフライン利用可能なコンテンツの場合には、利用回数制限、買い切りを示す記述がある。

【0071】(b) サービスプロバイダ(SP)用メモリ領域管理(確保)用属性証明書(AC)：ユーザデバイスにサービスプロバイダ(SP)を登録する場合、SPに関する情報格納領域をユーザデバイス内に確保する必要がある。この時の領域確保の許諾情報を属性証明書(AC)に格納し、ユーザデバイスでは、属性証明書(AC)に格納された情報を従って、ユーザデバイス内にSP用の領域を確保する。

【0072】(c) サービスプロバイダ(SP)用メモリ領域管理(削除)用属性証明書(AC)：ユーザデバイス内に確保したSP用領域の削除の許諾情報を格納した属性証明書(AC)である。ユーザデバイスでは、属性証明書(AC)に格納された情報を従って、ユーザデバイス内のSP用の領域の削除処理を実行する。

【0073】鍵データ：鍵データとしては、デバイスに対して設定される公開鍵、秘密鍵のペア、コンテンツ等のデータ保存の際の暗号処理用鍵として用いられるストレージ鍵、さらに、乱数生成用鍵、相互認証用鍵等が格

納される。

【0074】ストレージ鍵は、デバイスに保存するコンテンツ鍵の暗号化または復号化処理の少なくともいずれかに適用する鍵である。ストレージ鍵には、デバイス対応ストレージ鍵、サービスプロバイダ対応ストレージ鍵があり、サービスプロバイダ対応ストレージ鍵は、デバイスに登録された個々のサービスプロバイダ毎に各サービスプロバイダ管理領域内に格納される鍵であり、対応するサービスプロバイダの提供するコンテンツ鍵に対応して適用される。デバイス対応ストレージ鍵には、システムホルダと、デバイスのみが共有する鍵として構成されるグローバル共通鍵が含まれ、グローバル共通鍵は、サービスプロバイダにおける復号化処理を防止した暗号化コンテンツ鍵の配信処理を実行する際に用いられる。これらの鍵を適用した処理の詳細については後段で説明する。

【0075】識別情報：識別情報としては、ユーザデバイス自身の識別子としてのデバイスID、ユーザデバイスに登録したサービスプロバイダ(SP)の識別子としてのサービスプロバイダID、ユーザデバイスを利用するユーザに付与されたユーザID、なお、ユーザIDはサービスプロバイダ等、外部エンティティ毎に異なるユーザIDが付与可能である。アプリケーションIDは、サービスプロバイダ(SP)によって提供されるサービス、コンテンツに対応する識別情報としてのIDである。

【0076】その他：ユーザデバイスには、さらに、認証情報として、ユーザデバイス内に登録したサービスプロバイダ(SP)情報の利用許諾を得るための認証情報（例えばパスワード）が格納される。パスワードを入力することにより、ユーザデバイス内に登録したサービスプロバイダ(SP)情報の取得が可能となり、情報取得後、サービスプロバイダの提供するアプリケーション、コンテンツの利用が許可される。認証情報（パスワード）を忘れた場合には、マスターパスワードを用いて認証情報（パスワード）の初期化（リセット）処理が可能である。

【0077】さらに乱数生成用のシード情報が格納される。乱数は、認証処理、暗号処理等の際に、例えばANSIX9.17に従って生成する。

【0078】さらに、コンテンツ利用回数情報、あるいはコンテンツ利用回数情報に基づいて算出されるハッシュ値が格納される。これは、アプリケーション、コンテンツに対する属性証明書に格納された利用回数制限でのコンテンツ利用を厳格に実行するために必要となる情報であり、コンテンツに対する属性証明書の識別情報としてのアプリケーションID、属性証明書のシリアル番号、コンテンツの利用制限回数を保存する。署名付けやハッシュをとるだけでは改竄は可能であるが、検出できれば実質的に改竄できないことと同様の効果があ

る。

【0079】[ユーザデバイス内のメモリ構成] 不揮発性メモリの一形態であるフラッシュメモリ等のEEPROM(Electrically Erasable Programmable ROM)によって構成されるメモリ部206には、上述した様々なデータの少なくとも一部が格納されるが、これらは、メモリ部206領域に分割管理された3つの領域、すなわち、(1)デバイス管理領域、(2)システム管理領域、(3)サービス・プロバイダ管理領域に区分されて格納される。以下、これらの各領域毎の格納データについて説明する。

#### 【0080】(1) デバイス管理領域

デバイス管理領域は、デバイス固有のシステムに依存しない情報が保持されている。この領域はデバイス製造時に、最初に領域が確保され、不揮発性メモリの先頭の複数ブロックを占める領域である。デバイス管理領域では、少なくとも以下のデータを保持・管理する。

デバイスID

乱数生成用シード

20 乱数生成用暗号鍵

相互認証鍵

デバイス対応ストレージ鍵

【0081】相互認証鍵は、セキュリティチップ内のデータをセキュリティチップ外部に出力する場合等に出力先となるエンティティとの認証用の鍵である。なお、エンティティは、セキュリティチップを装着した例えはゲーム端末、DVD、CD等の再生装置、記録再生装置であるユーザデバイスも含む。セキュリティチップと、セキュリティチップを持つユーザデバイス間でのデータ転送、さらにはユーザデバイスを介した外部のサービスプロバイダとのデータ通信時などに相互認証鍵を適用した相互認証処理が実行される。相互認証の成立を条件として、相互認証時に生成したセッション鍵で暗号化してセキュリティチップ内部と外部間のデータ転送が実行される。

【0082】デバイス対応ストレージ鍵は、セキュリティチップ内部のデータを外部に保持する場合に、データを暗号化し、閲覧・改竄を防ぐための鍵である。デバイス・ストレージ鍵は、公開鍵系でも共通鍵系でもどちらでもよい。乱数生成用シードは、擬似乱数を算術演算により求める際に、初期シードとして用いるデータである。乱数生成用暗号鍵を用いて擬似乱数を算術演算して乱数を生成する。

【0083】共通鍵系デバイス対応ストレージ鍵には、システムホルダと、デバイスのみが共有する鍵として構成されるグローバル共通鍵が含まれ、グローバル共通鍵は、サービスプロバイダにおける復号化処理を防止した暗号化コンテンツ鍵の配信処理を実行する際に用いられる。グローバル共通鍵については、後段で詳細に説明する。

## 【0084】(2) システム管理領域

システム管理領域は、デバイス管理領域と同様にメモリ領域に確保される。システム管理領域では、以下のデータを保持・管理する。

ルート認証局（CA）公開鍵証明書

デバイス公開鍵証明書

デバイス秘密鍵

【0085】ルート認証局（CA）公開鍵証明書は、セキュリティチップ内の認証系すべての根源となる証明書で、他の証明書の署名検証を辿って、前述の連鎖検証を行なうと、最後にはルート認証局（CA）の公開鍵証明書に辿り着くことになる。

【0086】デバイス公開鍵証明書は、サービスプロバイダとの相互認証時に用いる公開鍵証明書である。デバイス秘密鍵を外部で生成し、インポートする場合には、デバイス公開鍵証明書も同時に生成される。デバイス側でデバイス秘密鍵・公開鍵を生成する場合には、デバイス内でデバイス秘密鍵・公開鍵が生成された後に、デバイス公開鍵がデバイスから読み出され、デバイス公開鍵証明書の発行処理を行ない、発行されたデバイス公開鍵証明書のインポートが行われる。

【0087】デバイス秘密鍵は、データに対して署名付けおよび認証するための鍵である。秘密鍵は、公開鍵とペアで生成されるが、予め外部で生成して、デバイスにセキュアにインポートする構成とするか、デバイス内部で生成し、決して外部に出さない構成とするかのいずれかの構成とする。

## 【0088】(3) サービスプロバイダ管理領域

サービスプロバイダ（SP）管理領域は、サービスプロバイダ（SP）管理テーブルとサービスプロバイダ（SP）管理情報とからなる。サービスプロバイダ（SP）管理テーブルは、サービスプロバイダ（SP）管理領域内で各サービスプロバイダ（SP）情報の所在を示すためのテーブルでありサービスプロバイダの識別子に対応させてメモリの各サービスプロバイダ（SP）情報の格納位置情報をを持つ。

【0089】なお、サービスプロバイダ（SP）管理領域には、ユーザデバイスがサービスプロバイダ（SP）毎に会員登録を行うことにより、サービスプロバイダ（SP）毎の領域がデバイス内のメモリ領域に確保される。なお、領域確保あるいは削除処理は、属性証明書の記述に基づいて実行される。サービスプロバイダ（SP）管理領域には、以下の情報を保持する。

【0090】サービスプロバイダ（SP）対応秘密鍵  
サービスプロバイダ（SP）対応ストレージ秘密鍵（公開鍵方式）

サービスプロバイダ（SP）対応ストレージ鍵（共通鍵方式）

外部管理情報のハッシュ値

コンテンツ利用回数管理データ

## 認証情報

## ユーザ情報

【0091】サービスプロバイダ（SP）対応秘密鍵は、登録サービスプロバイダ（SP）毎に対応して生成した登録サービスプロバイダ（SP）との相互認証処理または暗号化データ転送処理等に適用する公開鍵と秘密鍵のペアの秘密鍵である。登録サービスプロバイダ（SP）と、セキュリティチップとが相互認証する場合に必要とする鍵である。

10 【0092】サービスプロバイダ（SP）対応ストレージ秘密鍵（公開鍵方式）は、サービスプロバイダの提供するコンテンツ利用をオフラインで利用可能である場合、すなわち、取得したコンテンツを利用する毎にサービスプロバイダとの接続を必要としないコンテンツである場合、コンテンツに対応する暗号化コンテンツ鍵の復号用の鍵である。暗号化コンテンツ鍵は、サービスプロバイダ（SP）対応ストレージ秘密鍵に対応するサービスプロバイダ（SP）対応ストレージ公開鍵によってサービスプロバイダにおいて暗号化されて属性証明書（AC）に格納されてユーザデバイスに送信され、ユーザデバイスのセキュリティチップ内でサービスプロバイダ（SP）対応ストレージ秘密鍵で復号してコンテンツ鍵の取得が可能となる。

20 【0093】サービスプロバイダ（SP）対応ストレージ鍵（共通鍵方式）は、サービスプロバイダの提供するコンテンツ利用をオフラインで利用可能である場合、すなわち、取得したコンテンツを利用する毎にサービスプロバイダとの接続を必要としないコンテンツである場合、コンテンツに対応する暗号化コンテンツ鍵の復号用の鍵であり、暗号化、復号化処理に共通に適用可能な鍵である。なお、サービスプロバイダ（SP）対応ストレージ秘密鍵（公開鍵方式）と、サービスプロバイダ（SP）対応ストレージ鍵（共通鍵方式）は、いずれか一方のみを格納し適用する構成としてもよい。。

30 【0094】外部管理情報のハッシュ（Hash）値は、セキュリティチップ内部で管理するには大きすぎるデータを外部メモリの特定領域に出し、その領域のハッシュ値をセキュリティチップ内で管理することにより、改竄ができないようにするものである。例えば、コンテンツの回数利用制限をかける場合に、残回数などがハッシュ値による管理対象となる。回数管理コンテンツの場合、回数情報の閲覧自体は問題ないが、改竄は防がなくてはならない。署名付けやハッシュをとるだけでは改竄は可能であるが、検出できれば実質的に改竄できないことと同様の効果がある。

40 【0095】コンテンツ利用回数管理データ  
アプリケーション（コンテンツ）の利用可能回数をセキュリティチップがローカルで管理する場合がある。この時、セキュリティチップ内部では、アプリケーションID、属性証明書（AC）のシリアル、利用可能回数とを

保持・管理する。コンテンツ利用回数管理データの管理処理については、後段で詳細に説明する。

#### 【0096】認証情報

認証情報とは、サービスプロバイダ(SP)管理領域で管理される管理情報を保護する目的の情報である。ユーザはサービスプロバイダ(SP)接続時にはサービスプロバイダ(SP)との相互認証が必要となるが、相互認証に必要な情報は、サービスプロバイダ(SP)管理領域に格納される。この管理領域から必要情報を取得するために用いるのが認証情報である。認証情報は具体的には、例えばパスワードである。認証情報(パスワード)をユーザが忘れた場合には、サービスプロバイダ(SP)管理領域の管理情報の利用許諾が得られなくなる。この場合には、マスター・パスワードを入力することにより認証情報自体のリセット、または変更を行うことができる。これらの処理構成については、後段で詳細に説明する。

#### 【0097】ユーザ情報

ユーザ情報は、サービスプロバイダ(SP)により割り振られたユーザIDなどのユーザ固有情報である。

【0098】[パスワード管理]以下、図1に示すユーザデバイス101が、サービスプロバイダ(コンテンツディストリビュータ)102の提供するコンテンツを受領し、属性証明書に従った利用制限の下にコンテンツを利用する処理、およびコンテンツ利用に際して必要となる各種処理の詳細について説明する。まず、コンテンツを提供するサービスプロバイダに関する情報を格納したユーザデバイス内のメモリ領域のサービスプロバイダ管理領域へのアクセス制御用の認証情報(パスワード)について説明する。

#### 【0099】(1) 認証情報(パスワード)登録処理

ユーザデバイスを購入したユーザがシステムホルダの管理下にある様々なサービスプロバイダからコンテンツを購入する処理、あるいは購入したコンテンツを利用する処理を行なうためには、ユーザデバイス内のメモリ領域にサービスプロバイダ管理領域を設定し、このサービスプロバイダ管理領域にサービスプロバイダ毎の管理情報を格納する処理が必要となる。ユーザデバイス内のメモリ領域にサービスプロバイダ管理領域の設定されたサービスプロバイダを、以下登録サービスプロバイダと呼ぶ。サービスプロバイダ管理領域の設定には、前述の属性証明書を適用し、ユーザデバイスがサービスプロバイダから受信した属性証明書に基づいて、ユーザデバイス内のメモリ領域に属性証明書の記録に従ったサービスプロバイダ管理領域の設定処理を実行する。

【0100】サービスプロバイダ管理領域を持つ登録サービスプロバイダに対して、ユーザデバイスがアクセスしてコンテンツの購入、あるいは利用を行なうためには、先ず、ユーザデバイス内のサービスプロバイダ管理領域内的情報を取得することが必要となる。サービスプロ

バイダ管理領域には、ユーザデバイスとサービスプロバイダ間の相互認証処理に必要な情報が格納されており、これらの情報を取得してサービスプロバイダとの相互認証を行なうことが必要となるからである。

【0101】このサービスプロバイダ管理領域にアクセスするためにユーザは各登録サービスプロバイダ毎に設定される認証情報(パスワード)を、ユーザデバイスの入力手段を介して入力することが必要となる。なお、以下の説明において、「サービスプロバイダ毎に」との記述は、「各登録サービス毎かつ各ユーザ毎」と同義である。セキュリティチップ側で入力パスワードと登録パスワードの一一致検証を行ない、一致した場合に限り、セキュリティチップ内のメモリに形成されたサービスプロバイダ管理領域内の情報取得が可能となり、その後のサービスプロバイダとの相互認証処理、へのアクセスが可能となる。

【0102】認証情報(パスワード)は、ユーザデバイスに登録されたサービスプロバイダ毎に設定される。これらのパスワードの初期登録は、ユーザ自身が実行する。パスワードの初期登録処理について、図8を参照して説明する。図8のシーケンス図において、左側がセキュリティチップ、右側がセキュリティチップを持つユーザデバイスにおけるユーザインタフェース側処理である。

【0103】まず、(1)パスワード登録対象となる対応するサービスプロバイダを指定して認証情報(パスワード)初期登録処理開始要求をユーザが入力する。

(2)セキュリティチップ側では、ユーザの指定したサービスプロバイダが、セキュリティチップ内のメモリにすでに管理領域を設定済みの登録サービスプロバイダであり、パスワード設定されていない状態であるか等のステータス確認処理を行ない、これらが確認された場合に、(3)認証情報(パスワード)初期登録処理を許可する。

【0104】次に、ユーザはユーザインタフェース側からキーボード等の入力手段を介し、(4)パスワードを入力し、(5)セキュリティチップの制御部は入力された認証情報(パスワード)をテンポラリにメモリに保持し、(6)同一パスワードの再入力要求を行ない、

40 (7)ユーザにより認証情報(パスワード)の再入力がなされると、(8)セキュリティチップの制御部は再入力認証情報(パスワード)とテンポラリにメモリに保持してある認証情報(パスワード)の照合を実行し、照合が成立した場合には、(9)認証情報(パスワード)の書き込み処理を実行し、(10)書き込み結果をユーザに通知し、OKなら終了する。(11)NGの場合は、(1)の処理に戻る。

【0105】(2)認証情報(パスワード)変更処理  
図9および図10にパスワードの変更処理のシーケンス図を示す。パスワード変更は、登録済みパスワードを用

いた変更処理（通常時）と、マスターpasswordを用いた変更処理（緊急時）の2つの処理態様がある。

【0106】まず、図9のシーケンス図に基づいて、通常時のpassword変更処理、すなわち、登録済みpasswordを用いた変更処理について説明する。左側がセキュリティチップ、右側がセキュリティチップを持つユーザデバイスのユーザインタフェース側処理である。

【0107】まず、(1) password変更処理対象となる対応するサービスプロバイダを指定して認証情報(password)変更処理開始要求をユーザが入力する。

(2) セキュリティチップ側では、ユーザの指定したサービスプロバイダがメモリに管理領域を設定され登録済みのサービスプロバイダ(SP)であり、passwordの設定されたSPであるか等のステータス確認を処理を行ない、これらが確認されたことを条件として、(3) 登録済みの認証情報(password)入力要求を行なう。ユーザはユーザインタフェース側からキーボード等の入力手段を介し、(4) 登録済みpasswordを入力し、

(5) セキュリティチップの制御部は入力を確認すると、サービスプロバイダ管理領域に書き込まれている登録認証情報(password)との照合処理を実行する。

【0108】照合が成立すると、(6) 変更処理許可を通知する。ユーザはユーザインタフェース側からキーボード等の入力手段を介し、(7) 新たな認証情報(password)を入力し、(8) セキュリティチップの制御部は入力された認証情報(password)をテンポラリにメモリに保持し、(9) 同一passwordの再入力要求を行ない、(10) ユーザにより認証情報(password)の再入力がなされると、(11) セキュリティチップの制御部は再入力認証情報(password)とテンポラリにメモリに保持してある認証情報(password)の照合を実行し、照合が成立した場合には、(12) 認証情報(password)の書き込み処理を実行し、(13) 書き込み結果をユーザに通知し、OKなら終了する。(14) NGの場合は、(1) の処理に戻る。

【0109】(3) マスターpasswordを用いた認証情報(password)リセット処理

次に、図10のシーケンス図に基づいて、緊急時のpassword変更処理等において実行されるマスターpasswordを用いた認証情報(password)リセット処理について説明する。左側がセキュリティチップ、右側がセキュリティチップを持つユーザデバイスを装着した端末におけるユーザインタフェース側処理である。

【0110】まず、(1) password変更処理対象となる対応するサービスプロバイダを指定して認証情報(password)リセット処理開始要求をユーザが入力する。

(2) セキュリティチップ側では、ユーザの指定したサービスプロバイダがメモリに管理領域を設定され登録済みのサービスプロバイダ(SP)であり、passwordの設定されたSPであるか等のステータス確認を処理を行

ない、これらの条件を満足する場合に、(3) マスターpassword入力要求を行なう。ユーザはユーザインタフェース側からキーボード等の入力手段を介し、(4) マスターpasswordを入力し、(5) セキュリティチップの制御部は入力されたマスターpasswordの照合処理を実行し、正しいマスターpasswordの入力であるか否かを判定し、検証の結果、正しいマスターpassword入力であると判定すると、(6) サービスプロバイダ管理領域に書き込まれている登録認証情報(password)の初期化、すなわち登録済み認証情報(password)のリセット処理を実行する。

【0111】セキュリティチップの制御部は、リセット処理の後、(7) 処理結果通知をユーザに通知し、OKであれば、例えば、ユーザは前述の認証情報(password)登録処理を実行する。これらの処理は、先に図8を参照して説明した処理と同様であるので説明を省略する。(8) リセット処理結果がNGの場合は、(1) の処理に戻る。

【0112】図10の処理シーケンスを用いて説明したように、マスターpasswordは、各登録サービスプロバイダについて登録済みの認証情報(password)の初期化処理、すなわちリセットする際に適用される。マスターpasswordを用いた認証情報初期化(リセット)処理は、セキュリティチップに登録されたサービスプロバイダすべての認証情報に対して有効である。

【0113】図11にマスターpasswordと各登録サービスプロバイダの認証情報(password)との関係図を示す。図11に示すようにマスターpasswordは、各サービスプロバイダ対応認証情報に対する上位passwordとして存在し、マスターpasswordの入力により、各各登録サービスプロバイダの認証情報(password)の初期化(リセット)が実行され、新たな認証情報を各登録サービスプロバイダの認証情報(password)として再登録することが可能となる。

【0114】マスターpasswordは、図12に示すように、ユーザデバイスの購入時に例えばプリントされた用紙がデバイスに添付されて配布される。マスターpasswordはデバイスの製造時に工場で書き込まれるが、ユーザによるマスターpasswordのデバイスからの読み出しはできない構成となっている。マスターpasswordは、デバイスに固有の識別子であるデバイスIDと、マスターキーに基づいて生成される。マスターキーは情報処理装置個々または一群の情報処理装置に対応して設定されるキーである。

【0115】マスターpasswordをユーザが忘れた場合には、サポートセンターへの登録を条件としてマスターpasswordの再発行処理が可能となる。図13にサポートセンターへのユーザ登録処理および、マスターpasswordの再発行処理シーケンス図を示す。

【0116】図13の上段が、サポートセンターに対する

ユーザ登録処理シーケンス図を示す。ユーザは購入デバイスに添付された登録用紙の郵送、あるいはデバイスを設定した端末を介してサポートセンタに接続してユーザ登録を行なうことができる。ユーザ登録は、ユーザ住所、電話番号、デバイスのID等のデータをサポートセンタに登録する処理として実行され、サポートセンタにおいてユーザ登録が完了すると、ユーザ登録完了通知がサポートセンタからユーザに送付または送信される。

【0117】図13の下段が、ユーザがマスターpasswordを忘れた場合に、ユーザと、サポートセンタ間で実行されるマスターpassword再発行処理のシーケンスである。ユーザは、デバイスIDを伴うユーザ情報データとともに、マスターpasswordの再発行要求をサポートセンタに対して送信し、サポートセンタが要求を受信すると、サポートセンタは、ユーザ情報、ユーザIDが登録済みデータと一致するかを判定し、一致した場合は、ユーザデバイスIDに基づくマスターpasswordの検索あるいはマスターキーを用いたマスターpasswordの生成処理を実行する。サポートセンタは、情報処理装置としてのユーザデバイスに対応して設定されたデバイス識別子としてのデバイスIDと、マスターpasswordとを対応させたマスターpassword格納データベースを有する。あるいは、デバイスIDと、デバイス個々に固有のキー、または一群のデバイスに共通するキーとして設定されたマスターキーとを対応させたマスターキー格納データベースのいずれかを有し、マスターpassword格納データベースを有する場合には、デバイスIDに基づいてデータベース検索を実行してマスターpasswordを取得する。マスターキー格納データベースを有する場合には、デバイスIDに対する、マスターキーを適用した暗号処理によるマスターpassword生成処理を実行し、生成したマスターpasswordをユーザデバイスに送付する処理を実行する。

【0118】ユーザデバイスIDに基づくマスターキーによるマスターpasswordの生成処理フローを図14に示す。図14のフローについて説明する。まず、ステップS101において、マスターキーKm1を用いてデバイスIDの暗号化処理を実行する。その結果をステップS102において、MPaとする。さらに、結果MPaに対してマスターキーKm2を適用した暗号化処理を実行してpasswordMPを得て、ステップS103において、ASCIIコードに変換する。暗号化処理は例えばDES、トリブルDES等の暗号化アルゴリズムが適用可能である。マスターキーKm1、Km2は、複数のデバイスに対して共通に設定されたキーであり、サポートセンタはユーザデバイスIDに基づいて、サポートセンタで保持する複数のキーから適用すべきマスターキーを選択して使用する。

【0119】図13のシーケンス図に戻って説明を続ける。サポートセンタでマスターpasswordの生成が実行

されると、サポートセンタは、マスターpasswordをオンラインまたはオフラインでユーザまたはユーザデバイスに対して送信または送付する。

【0120】以上のシーケンスに従って、ユーザは、サポートセンタを利用してマスターpasswordの再発行処理を行なうことができる。なお、ユーザデバイスと、サポートセンタ間においては、データ送受信の前処理として相互認証処理を実行し、送受信する秘密データ、例えばユーザID、マスターpassword等は相互認証時に生成したセッションキーで暗号化し、またデータの改竄防止のために署名の生成、検証を行なうことが好ましい。なお、これら相互認証処理、署名生成、検証処理等の詳細については、コンテンツの配信処理の項目で詳しく説明する。

【0121】また、ユーザは、サポートセンタを利用したマスターpasswordの再発行処理をオフラインで行なうことも可能である。この場合は、ハガキなどに本人確認のための情報を記入して送付するなどの処理が行なわれることになる。

20 【0122】【コンテンツ配信処理】ユーザデバイス内のセキュリティチップ内のメモリ領域にサービスプロバイダの管理領域が登録され、サービスプロバイダとの認証に必要な情報、上記password等が登録されると、これらの情報を用いてサービスプロバイダとの通信によるコンテンツ購入が可能となる。以下、コンテンツ購入処理の詳細について説明する。

【0123】コンテンツ購入処理における概要を説明するシーケンス図を図15に示す。左側がセキュリティチップを持つユーザデバイス側処理であり、右側がサービスプロバイダ側処理である。

【0124】ユーザデバイスは、まず、コンテンツの購入要求をサービスプロバイダに出力する。サービスプロバイダがコンテンツ購入要求を受信すると、ユーザデバイスとサービスプロバイダ間において相互認証が実行される。相互認証が成立し、双方の正当性が確認されると、サービスプロバイダは、購入要求コンテンツに対応する属性証明書（AC：Attribute Certificate）を生成し、ユーザデバイスに送信する。属性証明書には、コンテンツを復号するためのコンテンツ鍵：Kcが暗号化されて格納され、また、利用回数、利用期限等のコンテンツ利用条件が記録されている。また格納データに対して属性証明書発行者である属性証明書認証局（AA：Attribute Certificate Authority）の署名がなされており、改竄防止を考慮したものとなっている。

【0125】属性証明書を受信したユーザデバイスは、属性証明書の署名検証処理を実行し、改竄なしの判定に基づいて属性証明書をメモリに保存する。さらに、ユーザデバイスは、コンテンツの要求をサービスプロバイダに対して行ない、サービスプロバイダは、先にユーザデバイスに送付した属性証明書内に格納されたコンテンツ

鍵：K<sub>c</sub>で暗号化したコンテンツをユーザデバイスに送付する。ユーザデバイス側では、属性証明書から取り出した暗号化されたコンテンツ鍵の復号化処理を実行してコンテンツ鍵を取り出し、取り出したコンテンツ鍵を適用した暗号化コンテンツの復号化処理によりコンテンツを取得し、利用する。なお、属性証明書に格納したコンテンツ鍵の復号化処理をサービスプロバイダ側で実行する態様（オンライン復号）もある。これらの具体的な処理例については、後段で説明する。

【0126】コンテンツ配信に伴う大まかな流れは、以上、図15を用いて説明した通りである。以下、各処理の詳細について説明する。なお、図15に示した処理シーケンスでは、コンテンツに対応する属性証明書を暗号化コンテンツ送付の前に実行しているが、暗号化コンテンツの配信と、属性証明書の配信はいずれが先でもよく、同時に配信する処理としてもよい。また、それをディスク等の記録媒体に格納して配信するオンライン配信を行なう構成とすることも可能である。

【0127】また、サービスプロバイダからユーザデバイスに対するコンテンツ配信あるいは属性証明書（A C : Attribute Certificate）の配信形態としては、ユーザ側からサービスプロバイダに対する要求に基づいて実行される形態と、ユーザの要求の有無に関係なく例えばサブスクリーパ契約を結んでいるユーザに対して、サービスプロバイダから一方的に送信するいわゆるプッシュ型の形態（プッシュ型モデル）のいずれの形態も可能である。プッシュ型モデルにおいては、サービスプロバイダが予め目標ユーザ向けの属性証明書（A C）を作成して配信することになる。

【0128】（1）相互認証処理、コンテンツの購入要求エンティティであるユーザデバイス、およびコンテンツの提供元であるサービスプロバイダ間では、まず相互認証処理が実行される。データ送受信を実行する2つの手段間では、相互に相手が正しいデータ通信者であるか否かを確認して、その後に必要なデータ転送を行なうことが行われる。相手が正しいデータ通信者であるか否かの確認処理が相互認証処理である。相互認証処理時にセッション鍵の生成を実行して、生成したセッション鍵を共有鍵として暗号化処理を実行してデータ送信を行なう構成が1つの好ましいデータ転送方式である。相互認証方式としては、公開鍵暗号方式、共通鍵暗号方式等、各方式の適用が可能である。

【0129】ここでは、公開鍵暗号方式の1つの認証処理方式であるハンドシェイクプロトコル（TLS 1.0）について図16のシーケンス図を参照して説明する。

【0130】図16において、左側がユーザデバイス（クライアント）の処理、右側がサービスプロバイダ（サーバ）側の処理を示している。まず、（1）サービスプロバイダ（サーバ）が暗号化仕様を決定するためのネゴ

シエーション開始要求をハローリクエストとしてユーザデバイス（クライアント）に送信する。（2）ユーザデバイス（クライアント）はハローリクエストを受信すると、利用する暗号化アルゴリズム、セッションID、プロトコルバージョンの候補をクライアントハローとして、サービスプロバイダ（サーバ）側に送信する。

【0131】（3）サービスプロバイダ（サーバ）側は、利用を決定した暗号化アルゴリズム、セッションID、プロトコルバージョンをサーバハローとしてユーザデバイス（クライアント）に送信する。（4）サービスプロバイダ（サーバ）は、自己の所有するルートCAまでの公開鍵証明書（X.509v3）一式をユーザデバイス（クライアント）に送信（サーバ・サーティフィケート）する。なお、証明書連鎖をたどって最上位の公開鍵証明書まで順に検証を実施しない場合には、必ずしもルートCAまでの公開鍵証明書（X.509v3）一式を送付する必要はない。（5）サービスプロバイダ（サーバ）は、RSA公開鍵またはDiffie & Hellman公開鍵情報をユーザデバイス（クライアント）に送信（サーバ・キー・エクスチェンジ）する。これは証明書が利用できない場合に一時的に適用する公開鍵情報である。

【0132】（6）次にサービスプロバイダ（サーバ）側は、ユーザデバイス（クライアント）に対してサーティフィケート・リクエストとして、ユーザデバイス（クライアント）の有する証明書を要求し、（7）サービスプロバイダ（サーバ）によるネゴシエーション処理の終了を知らせる（サーバハロー終了）。

【0133】（8）サーバハロー終了を受信したユーザデバイス（クライアント）は、自己の所有するルートCAまでの公開鍵証明書（X.509v3）一式をサービスプロバイダ（サーバ）に送信（クライアント・サーティフィケート）する。なお、公開鍵証明書の連鎖検証を行なわない場合は公開鍵証明書の一式送付は必須ではない。（9）ユーザデバイス（クライアント）は、48バイト乱数をサービスプロバイダ（サーバ）の公開鍵で暗号化してサービスプロバイダ（サーバ）に送信する。サービスプロバイダ（サーバ）、ユーザデバイス（クライアント）は、この値をもとに送受信データ検証処理のためのメッセージ認証コード：MAC（Message Authentication Code）生成用のデータ等を含むマスターシークレットを生成する。

【0134】（10）ユーザデバイス（クライアント）は、クライアント証明書の正しさを確認するため、ここまでメッセージのダイジェストをクライアントの秘密鍵で暗号化してサービスプロバイダ（サーバ）に送信（クライアントサーティフィケート確認）し、（11）先に決定した暗号化アルゴリズム、鍵利用の開始を通知（チェンジ・サイファー・スペック）し、（12）認証の終了を通知する。一方、（13）サービスプロバイダ

(サーバ) 側からユーザデバイス（クライアント）に対しても、先に決定した暗号化アルゴリズム、鍵利用の開始を通知（チェンジ・サイファー・スペック）し、(14) 認証の終了を通知する。

【0135】上記処理において決定された暗号化アルゴリズムに従ってユーザデバイス（クライアント）とサービスプロバイダ（サーバ）間のデータ転送が実行されることになる。

【0136】データ改竄の検証は、上述の認証処理でユーザデバイス（クライアント）とサービスプロバイダ（サーバ）間の合意のもとに生成されたマスターシークレットから算出されるメッセージ認証コード：MAC (Message Authentication Code) を各エンティティの送信データに付加することでメッセージの改竄検証を行なう。

【0137】図17にメッセージ認証コード：MAC (Message Authentication Code) の生成構成を示す。データ送信側は、送信データに対して、認証処理において生成したマスターシークレットに基づいて生成されるMACシークレットを付加し、これらの全体データからハッシュ値を計算し、さらにMACシークレット、パディング、ハッシュ値に基づいてハッシュ算出を行なってメッセージ認証コード（MAC）を生成する。この生成したMACを送信データに付加して、受信側で受信データに基づいて生成したMACと受信MACとの一致が認められればデータ改竄なしと判定し、一致が認められない場合には、データの改竄があったものと判定する。

【0138】(2) コンテンツ利用権限情報証明書（属性証明書）の生成、送信

ユーザデバイスからコンテンツの要求がなされたサービスプロバイダは、要求コンテンツの復号化処理に適用可能なコンテンツ鍵：Kcを暗号化して格納し、コンテンツの利用制限情報を格納したコンテンツ利用権限情報証明書、例えば属性証明書（AC）を生成して、ユーザに対して送信する。

【0139】コンテンツ利用権限情報証明書、例えば属性証明書（AC）を生成する主体は、サービスプロバイダ自身であっても、またコンテンツ管理を実行する外部エンティティであってもよい。外部エンティティが属性証明書（AC）を生成する場合は、サービスプロバイダの要求に従ってその外部エンティティが属性証明書（AC）を生成する。

【0140】属性証明書には対応暗号化コンテンツの復号に適用可能なコンテンツ鍵：Kcが暗号化されて格納される。コンテンツ鍵Kcの暗号化に適用する鍵には、例えば、

(a) ユーザデバイスのセキュリティチップの各サービスプロバイダ管理領域に格納されたSP対応ストレージ秘密鍵に対応するサービスプロバイダ（SP）対応ストレージ公開鍵：SC. St o p u b. S P. K

(b) サービスプロバイダの保有する秘密鍵（共通鍵系）：S P. S t o . K

(c) システムホルダ（SH）とユーザデバイスで共有する鍵として生成されるグローバル共通鍵：Kgの各態様がある。なお、この他にも、いくつかの態様が可能である。例えばサービスプロバイダの保有する公開鍵で暗号化することも可能である。この場合は、ユーザデバイスから属性証明書（AC）を受信してサービスプロバイダの保有する秘密鍵で復号化することになる。

10 【0141】なお、いずれの暗号化態様を適用した場合でも、サービスプロバイダからユーザデバイスに対するコンテンツ配信あるいは属性証明書（AC：Attribute Certificate）の配信形態としては、ユーザ側からサービスプロバイダに対する要求に基づいて実行される形態と、ユーザの要求の有無に関係なく例えばサブスクリバ契約を結んでいるユーザに対して、サービスプロバイダから一方的に送信するいわゆるプッシュ型の形態（プッシュ型モデル）のいずれの形態も可能である。プッシュ型モデルにおいては、サービスプロバイダが予め目標ユーザ向けの属性証明書（AC）を作成して配信することになる。以下、上記(a)～(c)の態様における処理の詳細について説明する。

【0142】(a) SP対応ストレージ秘密鍵に対応するサービスプロバイダ（SP）対応ストレージ公開鍵：SC. St o p u b. S P. Kを適用した場合

前述したユーザデバイスのセキュリティチップのメモリ領域についての説明中で示したように、ユーザデバイスに登録された各登録サービスプロバイダについては、メモリに形成された各サービスプロバイダ管理領域にSP対応ストレージ秘密鍵：SC. St o p r i. S P. Kが格納される。ユーザデバイスのセキュリティチップでは、サービスプロバイダから提供されるコンテンツに対応する属性証明書の中からSP対応ストレージ秘密鍵に対応するサービスプロバイダ（SP）対応ストレージ公開鍵：SC. St o p u b. S P. Kで暗号化されたコンテンツ鍵：Kc、すなわち、[SC. St o p u b. S P. K (Kc)]を取り出して、SP対応ストレージ秘密鍵：SC. St o p r i. S P. Kで復号化処理を実行することにより、コンテンツ鍵：Kcを取得する。

40 40 【A (B)】は、Aで暗号化されたBからなるデータを示すものとする。本形態では、ユーザデバイスは、コンテンツの利用時、すなわち復号時にサービスプロバイダと接続することなくユーザデバイス内の処理としてコンテンツ復号、すなわちオフライン復号が可能となる。

【0143】なお、上記例では、公開鍵暗号方式を適用し、コンテンツ鍵の暗号化にSP対応ストレージ公開鍵：SC. St o p u b. S P. Kを用い、コンテンツ鍵の復号にSP対応ストレージ秘密鍵：SC. St o p r i. S P. Kを用いた構成例について説明したが、共

通鍵方式を適用することも可能であり、共通鍵方式を適用する場合は、コンテンツ鍵の暗号化、復号化の双方の処理に S P 対応ストレージ鍵（共通鍵）：S C, S t o, S P, K を用いる。この場合、S P 対応ストレージ鍵（共通鍵）：S C, S t o, S P, K は、セキュリティチップのメモリの対応するサービスプロバイダのサービスプロバイダ管理領域に格納する。

【0144】(b) サービスプロバイダの保有する秘密鍵（共通鍵系）：S P, S t o, K を適用した場合  
サービスプロバイダは、ユーザデバイスに対して提供するコンテンツに対応して設定される属性証明書に格納するコンテンツ鍵：K c をサービスプロバイダが保有する秘密鍵：S P, S t o, K を適用して暗号化する。ユーザデバイスは、属性証明書を受信しても、属性証明書に格納された暗号化コンテンツ鍵：[S P, S t o, K (K c)] を復号することはできない。サービスプロバイダの保有する秘密鍵：S P, S t o, K はユーザデバイスは保有していないからである。

【0145】従って、コンテンツを利用（復号化）するためには、次のような処理が必要となる。まず、ユーザデバイスは、サービスプロバイダに属性証明書を送付してコンテンツ鍵の復号要求を行ない、サービスプロバイダにおいては、サービスプロバイダの保有する秘密鍵：S P, S t o, K によってコンテンツ鍵：K c の復号化を行なう。ユーザデバイスはサービスプロバイダより復号化されたコンテンツ鍵：K c を取得し、該コンテンツ鍵：K c で暗号化コンテンツの復号を行なう。本形態では、上述の(a)の形態と異なり、ユーザデバイスは、コンテンツの利用時、すなわち復号時にサービスプロバイダと接続することが必須となる。すなわちオンライン処理が必要となる。

【0146】(c) システムホルダ(S H)とユーザデバイスで共有する鍵として生成されるグローバル共通鍵：K g を適用した場合  
このグローバル共通鍵を利用する形態は、コンテンツの配信を実行するサービスプロバイダにおいて、システムホルダの許可なくコンテンツが配布、利用されることを防止し、システムホルダ(S H)による管理されたコンテンツ配信を行なうための構成である。サービスプロバイダに対してコンテンツを提供するコンテンツクリエータの有するコンテンツ製作者鍵、コンテンツ配信を行なうサービスプロバイダの有するコンテンツ配信者鍵、そしてシステムホルダ(S H)とユーザデバイスで共有する鍵として生成されるグローバル共通鍵：K g の各鍵を組み合わせた暗号化処理を行なった暗号化鍵データを属性証明書に格納し、コンテンツ利用者としてのエンティティであるユーザデバイスに配布することで、サービスプロバイダ自体もコンテンツ鍵を取り出すことを防止し、ユーザデバイスにおいてのみコンテンツ鍵：K c を取り出すことを可能とした構成である。

【0147】以下、これらの各形態について詳細に説明する。まず、上記(a)～(c)に共通する属性証明書の発行処理シーケンスについて図18を用いて説明する。

【0148】図18の処理シーケンスは、先に説明した図15のコンテンツ購入処理シーケンスの一部として構成される属性証明書の生成、送信処理を詳細に説明したものである。ユーザデバイスはセキュリティチップを内蔵し、セキュリティチップ内のメモリにはサービスプロバイダ管理領域が生成されており、サービスプロバイダ管理情報が格納済みであるとする。

【0149】図18の処理について説明する。ユーザデバイスとサービスプロバイダ間の相互認証が成立後、

(1) セキュリティチップを持つユーザデバイスは、サービスプロバイダに対して属性証明書(AC)の要求を行なう。属性証明書(AC)要求には、サービスプロバイダ管理領域に登録されたユーザID、コンテンツの指定識別子としてのアプリケーションID、さらにユーザが選択した利用条件データにユーザの秘密鍵(サービスプロバイダ対応秘密鍵)で署名したデータにユーザの公開鍵証明書(PKC)を添付して送信する。利用条件データは、例えばコンテンツ利用制限回数、利用期限等の指定データであり、ユーザによって選択可能である場合にユーザ指定データとして含まれる。

【0150】署名は、データ改竄の検証を可能とするために付加されるものであり、前述のMAC値を用いることも可能であり、公開鍵暗号方式を用いた電子署名を適用することも可能である。

【0151】公開鍵暗号方式を用いた電子署名の生成方法について、図19を用いて説明する。図19に示す処理は、E C - D S A ((Elliptic Curve Digital SignatureAlgorithm)、IEEE P1363/D3)を用いた電子署名データの生成処理フローである。なお、ここでは公開鍵暗号として楕円曲線暗号(Elliptic Curve Cryptosystem(以下、ECCと呼ぶ))を用いた例を説明する。なお、本発明のデータ処理装置においては、楕円曲線暗号以外にも、同様の公開鍵暗号方式における、例えばR S A暗号(Rivest, Shamir, Adleman)など(ANSI X9.31)を用いることも可能である。

【0152】図19の各ステップについて説明する。ステップS1において、pを標数、a, bを楕円曲線の係数(楕円曲線： $y^2 = x^3 + ax + b$ ,  $4a^3 + 27b^2 \neq 0$  (mod p))、Gを楕円曲線上のベースポイント、rをGの位数、K sを秘密鍵( $0 < K_s < r$ )とする。ステップS2において、メッセージMのハッシュ値を計算し、 $f = \text{Hash}(M)$ とする。

【0153】ここで、ハッシュ関数を用いてハッシュ値を求める方法を説明する。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関

数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、MD4、MD5、SHA-1などが用いられる場合もあるし、DES-CBCが用いられる場合もある。この場合は、最終出力値となるMAC（チェック値：ICVに相当する）がハッシュ値となる。

【0154】続けて、ステップS3で、乱数u（ $0 < u < r$ ）を生成し、ステップS4でベースポイントをu倍した座標V（Xv, Yv）を計算する。なお、楕円曲線上の加算、2倍算は次のように定義されている。

【0155】

【数1】P=(Xa, Ya), Q=(Xb, Yb), R=(Xc, Yc)=P+Qとすると、

P≠Qの時（加算）、

$$Xc = \lambda^2 - Xa - Xb$$

$$Yc = \lambda \times (Xa - Xc) - Ya$$

$$\lambda = (Yb - Ya) / (Xb - Xa)$$

P=Qの時（2倍算）、

$$Xc = \lambda^2 - 2Xa$$

$$Yc = \lambda \times (Xa - Xc) - Ya$$

$$\lambda = (3(Xa)^2 + a) / (2Ya)$$

【0156】これらを用いて点Gのu倍を計算する（速度は遅いが、最もわかりやすい演算方法として次のように行う。G、 $2 \times G$ 、 $4 \times G \dots$ を計算し、uを2進数展開して1が立っているところに対応する $2^i \times G$ （Gをi回2倍算した値（iはuのLSBから数えた時のビット位置））を加算する。

【0157】ステップS5で、 $c = Xv \bmod r$ を計算し、ステップS6でこの値が0になるかどうか判定し、0でなければステップS7で $d = [(f + cKs) / u] \bmod r$ を計算し、ステップS8でdが0であるかどうか判定し、dが0でなければ、ステップS9でcおよびdを電子署名データとして出力する。仮に、rを160ビット長の長さであると仮定すると、電子署名データは320ビット長となる。

【0158】ステップS6において、cが0であった場合、ステップS3に戻って新たな乱数を生成し直す。同様に、ステップS8でdが0であった場合も、ステップS3に戻って乱数を生成し直す。

【0159】次に、公開鍵暗号方式を用いた電子署名の検証方法を、図20を用いて説明する。ステップS11で、Mをメッセージ、pを標数、a, bを楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ,  $4a^3 + 27b^2 \neq 0 \pmod p$ ）、Gを楕円曲線上のベースポイント、rをGの位数、KsおよびGs×Gを公開鍵（ $0 < Ks < r$ ）とする。ステップS12で電子署名データcおよびdが $0 < c < r$ ,  $0 < d < r$ を満たすか検証する。これ

を満たしていた場合、ステップS13で、メッセージMのハッシュ値を計算し、 $f = \text{Hash}(M)$ とする。次に、ステップS14で $h = 1/d \bmod r$ を計算し、ステップS15で $h_1 = f \cdot h \bmod r$ ,  $h_2 = c \cdot h \bmod r$ を計算する。

【0160】ステップS16において、既に計算した $h_1$ および $h_2$ を用い、点 $P = (X_p, Y_p) = h_1 \times G + h_2 \cdot K_s \times G$ を計算する。電子署名検証者は、ベースポイントGおよび $K_s \times G$ を知っているので、図19のステップS4と同様に楕円曲線上の点のスカラーバイ倍の計算ができる。そして、ステップS17で点Pが無限遠点かどうか判定し、無限遠点でなければステップS18に進む（実際には、無限遠点の判定はステップS16でできてしまう。つまり、 $P = (X, Y)$ 、 $Q = (X, -Y)$ の加算を行うと、入力が計算できず、 $P + Q$ が無限遠点であることが判明している）。ステップS18で $X_p \bmod r$ を計算し、電子署名データcと比較する。最後に、この値が一致していた場合、ステップS19に進み、電子署名が正しいと判定する。

【0161】電子署名が正しいと判定された場合、データは改竄されておらず、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したことがわかる。

【0162】ステップS12において、電子署名データcまたはdが、 $0 < c < r$ ,  $0 < d < r$ を満たさなかった場合、ステップS20に進む。また、ステップS17において、点Pが無限遠点であった場合もステップS20に進む。さらにまた、ステップS18において、 $X_p \bmod r$ の値が、電子署名データcと一致していないかった場合にもステップS20に進む。

【0163】ステップS20において、電子署名が正しくないと判定された場合、データは改竄されているか、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したのではないことがわかる。上述したように、署名付けやハッシュをとるだけでは改竄は可能であるが、検出により実質的に改竄できないことと同様の効果がある。

【0164】属性証明書(AC)要求を受信したサービスプロバイダは、上述の署名検証処理等によって要求データに改竄がないことを確認すると、アプリケーションIDで特定されるコンテンツに対応するコンテンツ鍵：Kcを暗号化する。このコンテンツ鍵：Kcの暗号化に適用する鍵は、前述の(a)ユーザデバイスのセキュリティチップの各サービスプロバイダ管理領域に格納されたSP対応ストレージ秘密鍵：SC\_S\_topri\_SP\_K、(b)サービスプロバイダの保有する秘密鍵：SP\_Sto\_K、(c)システムホルダ(SH)とユーザデバイスで共有する鍵として生成されるグローバル共通鍵：Kgのいずれかである。

【0165】さらに、サービスプロバイダは、コンテンツの利用条件データ他の必要データを格納し、前述した図5に示す属性証明書を生成する。生成した属性証明書

には、サービスプロバイダの秘密鍵を用いた電子署名が付加される。電子署名の生成処理は、図19の処理フローと同様の処理に従って実行される。サービスプロバイダによって生成された属性証明書はユーザデバイスに送付され、ユーザデバイスにおいて、上述の図20の処理フローと同様のシーケンスに従って署名検証処理を実行する。

【0166】さらに、必要に応じてユーザデバイスは、属性証明書(AC)内のAC保持者の公開鍵証明書情報に従ってリンクする公開鍵証明書を取得して、公開鍵証明書の検証を行なうことが好ましい。例えば属性証明書(AC)の発行者の信頼度が不確かである場合には、属性証明書(AC)の発行者の公開鍵証明書の検証を行なうことによって、認証局の公開鍵証明書を正当に有しているか否かの判定が可能となる。なお、公開鍵証明書が前述したように階層構成をなしている場合は、経路を上位に辿って連鎖的な検証を行ない、ルート認証局(CA)の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【0167】属性証明書(AC)と公開鍵証明書(PKC)との関連確認処理、および各証明書の検証処理の詳細について、図を参照して説明する。図21のフローは、属性証明書(AC)の検証を実行する際に行なわれる属性証明書(AC)に関連する公開鍵証明書(PKC)の確認処理である。

【0168】確認対象の属性証明書(AC)がセット(S21)されると、属性証明書のAC保持者の公開鍵証明書情報(holder)フィールドを抽出(S22)し、抽出した公開鍵証明書情報(holder)フィールド内に格納された公開鍵証明書の発行者情報(PKC issuer)、公開鍵証明書シリアル番号(PKC serial)を確認(S23)し、公開鍵証明書の発行者情報(PKC issuer)、公開鍵証明書シリアル番号(PKC serial)に基づいて公開鍵証明書(PKC)を検索(S24)して、属性証明書(AC)に関連付けられた公開鍵証明書(PKC)を取得(S25)する。

【0169】図21に示すように、属性証明書(AC)と公開鍵証明書(PKC)とは、属性証明書に格納された公開鍵証明書情報(holder)フィールド内の公開鍵証明書発行者情報(PKC issuer)、および公開鍵証明書シリアル番号(PKC serial)により関連付けがなされている。

【0170】次に、図22を参照して公開鍵証明書(PKC)の検証処理について説明する。図22に示す公開鍵証明書(PKC)の検証は、下位から上位へ証明書連鎖をたどって最上位の公開鍵証明書までの連鎖情報を取得して、最上位(ルートCA)までの公開鍵証明書の署名検証を行なう連鎖検証処理フローである。まず、検証対象となる公開鍵証明書(PKC)をセット(S31)

し、公開鍵証明書(PKC)格納情報に基づいて、公開鍵証明書(PKC)署名者を特定(S32)する。さらに、検証対象となる証明書連鎖の最上位の公開鍵証明書であるかを判定(S33)し、最上位でない場合は、最上位公開鍵証明書を直接あるいはリポジトリなどから取得(S34)する。最上位公開鍵証明書が取得されセット(S35)されると、署名検証に必要な検証鍵(公開鍵)を取得(S36)し、検証対象の署名が自己署名であるか否かを判定し(S37)、自己署名でない場合は、下位PKCをセット(S39)して、上位の公開鍵証明書から取得した検証鍵(公開鍵)に基づいて署名検証を実行(S40)する。なお、ステップS37における自己署名判定において、自己署名の場合は自己の公開鍵を検証鍵とした検証を実行(S38)し、ステップS41に進む。

【0171】署名検証に成功した場合(S41: Yes)は、目的とするPKCの検証が完了したか否かを判定(S42)し、完了している場合は、PKC検証を終了する。完了していない場合は、ステップS36に戻り、署名検証に必要な検証鍵(公開鍵)の取得、下位の公開鍵証明書の署名検証を繰り返し実行する。なお、署名検証に失敗した場合(S41: No)は、ステップS43に進み、エラー処理、例えばその後の手続きを停止する等の処理を実行する。

【0172】次に、図23を参照して属性証明書(AC)の検証処理(例1)について説明する。まず、検証対象となる属性証明書(AC)をセット(S51)し、属性証明書(AC)格納情報に基づいて、属性証明書(AC)の所有者および署名者を特定(S52)する。さらに、属性証明書(AC)の所有者の公開鍵証明書を直接あるいはリポジトリなどから取得(S53)して、公開鍵証明書の検証処理を実行(S54)する。

【0173】公開鍵証明書の検証に失敗した場合(S55でNo)は、ステップS56に進み、エラー処理を行なう。例えばその後の処理を中止する。公開鍵証明書の検証に成功した場合(S55でYes)は、属性証明書(AC)の署名者に対応する公開鍵証明書を直接あるいはリポジトリなどから取得(S57)して、公開鍵証明書の検証処理を実行(S58)する。公開鍵証明書の検証に失敗した場合(S59でNo)は、ステップS60に進み、エラー処理を行なう。例えばその後の処理を中止する。公開鍵証明書の検証に成功した場合(S59でYes)は、属性証明書(AC)の署名者に対応する公開鍵証明書から公開鍵を取り出し(S61)て、取り出した公開鍵を用いて属性証明書(AC)の署名検証処理を実行(S62)する。署名検証に失敗した場合(S63でNo)は、ステップS64に進み、エラー処理を行なう。例えばその後の処理を中止する。署名検証に成功した場合(S63でYes)は、属性証明書検証を終了し、その後の処理、例えば属性証明書内の暗号化コンテ

ンツ鍵の取得等に移行する。

【0174】次に、図24を参照して属性証明書(AC)の検証処理(例2)について説明する。本例は、自デバイス内に属性証明書(AC)の検証処理に必要となる公開鍵証明書が格納されているか否かを判定し、公開鍵証明書が格納されている場合は、その検証を省略することとした例である。まず、検証対象となる属性証明書(AC)をセット(S71)し、属性証明書(AC)格納情報に基づいて、属性証明書(AC)の所有者および署名者を特定(S72)する。さらに、属性証明書(AC)の所有者の公開鍵証明書(PKC)が自デバイス内のメモリに格納保存されていないかを検索(S73)する。保存されている場合(S74でYes)は、属性証明書(AC)の所有者の公開鍵証明書を取り出し(S75)て、ステップS81に進む。

【0175】属性証明書(AC)の所有者の公開鍵証明書(PKC)が自デバイス内のメモリに保存されていない場合(S74でNo)は、属性証明書(AC)の所有者の公開鍵証明書(PKC)を直接あるいはリポジトリなどから取得(S76)して、属性証明書(AC)の所有者の公開鍵証明書(PKC)の検証処理を実行(S77)する。公開鍵証明書の検証に失敗した場合(S78でNo)は、ステップS79に進み、エラー処理を行なう。例えばその後の処理を中止する。公開鍵証明書の検証に成功した場合(S78でYes)は、公開鍵証明書の検証結果を保存(S80)した後、属性証明書(AC)の署名者に対応する公開鍵証明書(PKC)が自デバイス内のメモリに格納保存されていないかを検索(S81)する。保存されている場合(S82でYes)は、属性証明書(AC)の署名者の公開鍵証明書を取り出し(S83)て、ステップS88に進む。

【0176】属性証明書(AC)の署名者の公開鍵証明書(PKC)が自デバイス内のメモリに保存されていない場合(S82でNo)は、属性証明書(AC)の署名者の公開鍵証明書(PKC)を直接あるいはリポジトリなどから取得(S84)して、属性証明書(AC)の署名者の公開鍵証明書(PKC)の検証処理を実行(S85)する。公開鍵証明書の検証に失敗した場合(S86でNo)は、ステップS87に進み、エラー処理を行なう。例えばその後の処理を中止する。公開鍵証明書の検証に成功した場合(S86でYes)は、公開鍵証明書から属性証明書(AC)の署名検証に適用する鍵(公開鍵)を取り出し(S88)、属性証明書(AC)の署名検証処理を実行(S89)する。署名検証に失敗した場合(S90でNo)は、ステップS91に進み、エラー処理を行なう。例えばその後の処理を中止する。署名検証に成功した場合(S90でYes)は、属性証明書検証を終了し、その後の処理、例えば属性証明書内の暗号化コンテンツ鍵の取得等に移行する。

【0177】ユーザデバイスによる属性証明書の検証が

なされると、属性証明書はユーザデバイス内のセキュリティチップのメモリ、あるいはセキュリティチップ外のユーザデバイス制御部の管理下の外部メモリに格納され、コンテンツの利用時に、属性証明書内の暗号化コンテンツ鍵の取得、復号化処理を実行することになる。属性証明書から暗号化されたコンテンツ鍵を取得して復号する処理について、以下説明する。

【0178】(a) SP対応ストレージ秘密鍵に対応するサービスプロバイダ(SP)対応ストレージ公開鍵：SC. Stopub. SP. Kを適用した場合

まず、前述の(a) SP対応ストレージ秘密鍵に対応するサービスプロバイダ(SP)対応ストレージ公開鍵：SC. Stopub. SP. Kをコンテンツ鍵：Kcの暗号化に適用し、[SC. Stopub. SP. K (Kc)]を格納した属性証明書に基づくコンテンツ利用処理について説明する。

【0179】SP対応ストレージ秘密鍵：SC. Stopri. SP. Kは、サービスプロバイダ管理領域に格納され、ユーザは前述した認証情報(パスワード)入力により、この鍵を取り出して利用することができる。従って、コンテンツ鍵：Kcはサービスプロバイダに接続することなくオフライン処理として取得可能であり、コンテンツの復号が可能となる。

【0180】図25に属性証明書からの暗号化コンテンツ鍵取得、復号、コンテンツ鍵によるコンテンツ復号化処理のシーケンスを説明する図を示す。

【0181】図25のシーケンス図に従って説明する。図25は左からセキュリティチップ内部のメモリ、セキュリティチップ制御部、ユーザデバイス制御部の処理を示している。まず、ユーザデバイスに対してユーザの入力したコンテンツ識別情報としてのアプリケーションIDをセキュリティチップ制御部に送信し、メモリからアプリケーションIDに対応する属性証明書(AC)を取得する。ユーザデバイスでは、アプリケーションIDに対応する属性証明書であるかの検証を行ない、セキュリティチップ制御部に属性証明書をセットし、コンテンツ鍵：Kcの取得(復号)処理を要求する。

【0182】セキュリティチップ制御部は、属性証明書の署名検証を実行し、データ改竄のないことを確認し、

属性証明書内に格納された暗号化コンテンツ鍵：[SC. Stopub. SP. K (Kc)]を取り出して、サービスプロバイダ管理領域に格納されたSP対応ストレージ秘密鍵：SC. Stopri. SP. Kを適用して復号化処理を実行し、コンテンツ鍵：Kcを取得する。コンテンツ鍵：Kcの取得に成功すると、セキュリティチップ制御部は、ユーザデバイス制御部にコンテンツの復号準備が完了したことを通知する。

【0183】次にユーザデバイス制御部は、取得したコンテンツ鍵を適用して復号すべき暗号化コンテンツを、セキュリティチップ制御部を介してメモリから取得す

る。暗号化コンテンツがセキュリティチップ内のメモリではなく、外部メモリ（例えばハードディスク）等に格納されている場合は、外部メモリから暗号化コンテンツを取得する。さらに、取得した暗号化コンテンツをセキュリティチップに送信し、セキュリティチップ内で暗号化コンテンツに対してコンテンツ鍵：Kc を適用した復号化処理を実行し、復号化処理結果として得られるコンテンツをユーザデバイス制御部に出力する。

【0184】なお、上記構成例では、公開鍵暗号方式を適用し、コンテンツ鍵の暗号化に SP 対応ストレージ公開鍵：SC. Stopub. SP. K を用い、暗号化コンテンツ鍵の復号に SP 対応ストレージ秘密鍵：SC. Stopri. SP. K を用いた構成としたが、共通鍵方式を適用することも可能であり、共通鍵方式を適用する場合は、コンテンツ鍵の暗号化、復号化の双方の処理に SP 対応ストレージ鍵（共通鍵）：SC. Sto. SP. K を用いる。この場合、SP 対応ストレージ鍵（共通鍵）：SC. Sto. SP. K は、セキュリティチップのメモリの対応するサービスプロバイダのサービスプロバイダ管理領域に格納される。

【0185】(b) サービスプロバイダの保有する秘密鍵（共通鍵系）：SP. Sto. K を適用した場合  
次に、前述の (b) サービスプロバイダの保有する秘密鍵：SP. Sto. K をコンテンツ鍵：Kc の暗号化に適用し、[SP. Sto. K (Kc)] を格納した属性証明書に基づくコンテンツ利用処理について説明する。

【0186】サービスプロバイダの保有する秘密鍵：SP. Sto. K は、サービスプロバイダが保有し、ユーザデバイスには格納されていない鍵である。従って、ユーザデバイスがコンテンツ鍵：Kc を取得するためには、サービスプロバイダに接続して、コンテンツ鍵の復号化処理をサービスプロバイダに対して要求することが必要となり、オンライン処理によるコンテンツ復号を実行することとなる。

【0187】図26に属性証明書からのコンテンツ鍵取得、復号、コンテンツ鍵によるコンテンツ復号化処理のシーケンスを説明する図を示す。

【0188】図26のシーケンス図に従って説明する。  
図26は左からセキュリティチップ内部のメモリ、セキュリティチップ制御部、ユーザデバイス制御部、サービスプロバイダにおける処理を示している。

【0189】まず、ユーザデバイスに対してユーザの入力したコンテンツ識別情報としてのアプリケーションIDをセキュリティチップ制御部に送信し、メモリからアプリケーションIDに対応する属性証明書（AC）を取得する。ユーザデバイスでは、アプリケーションIDに対応する属性証明書であるかの検証を行ない、セキュリティチップ制御部に属性証明書をセットし、コンテンツ鍵：Kc の取得（復号）処理を要求する。

【0190】セキュリティチップ制御部は、属性証明書

の検証の後、属性証明書の発行元であるサービスプロバイダに対してユーザデバイスを介して接続し、セキュリティチップとサービスプロバイダ間の相互認証処理を実行する。この相互認証処理は、先に説明した図16のTLS1.0処理または、その他の方式、例えば公開鍵方式による相互認証処理として実行される。この相互認証処理においては、相互の公開鍵証明書の検証がなされ、必要に応じてルート認証局（CA）までの公開鍵証明書が連鎖的に検証される。この認証処理において、セキュリティチップと、サービスプロバイダはセッション鍵（Kses）を共有する。

【0191】相互認証が成立すると、セキュリティチップの制御部は、サービスプロバイダに対して属性証明書を送付する。属性証明書には、サービスプロバイダの保有する秘密鍵：SP. Sto. K で暗号化されたコンテンツ鍵のデータ、すなわち、[SP. Sto. K (Kc)] が格納されている。

【0192】セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、サービスプロバイダは、自己の所有する秘密鍵：SP. Sto. K を用いて、属性証明書に格納された暗号化コンテンツ鍵：[SP. Sto. K (Kc)] の復号化処理を実行し、コンテンツ鍵：Kc を取り出す。さらに、取り出したコンテンツ鍵：Kc を先の相互認証処理において生成したセッションキー（Kses）で暗号化して、ユーザデバイスのセキュリティチップに対して送信する。

【0193】セキュリティチップの制御部は、サービスプロバイダからセッションキーで暗号化されたコンテンツ鍵、すなわち、[Kses (Kc)] を受信すると、相互認証時に保有したセッションキーを用いて復号化処理を実行してコンテンツ鍵：Kc を取得する。

【0194】コンテンツ鍵：Kc の取得に成功すると、セキュリティチップ制御部は、ユーザデバイス制御部にコンテンツの復号準備が完了したことを通知する。次にユーザデバイス制御部は、取得したコンテンツ鍵を適用して復号すべき暗号化コンテンツをセキュリティチップ制御部を介してメモリから取得する。暗号化コンテンツがセキュリティチップ内のメモリではなく、外部メモリ（例えばハードディスク）等に格納されている場合は、外部メモリから暗号化コンテンツを取得する。さらに、取得した暗号化コンテンツをセキュリティチップに送信し、セキュリティチップ内で暗号化コンテンツに対してコンテンツ鍵：Kc を適用した復号化処理を実行し、復号化処理結果として得られるコンテンツをユーザデバイス制御部に出力する。

40  
45  
50

【0195】(c) システムホルダ(SH)とユーザデバイスで共有する鍵として生成されるグローバル共通鍵: Kg を適用した場合

次に、システムホルダ(SH)とユーザデバイスで共有する鍵として生成されるグローバル共通鍵: Kg を、コンテンツ鍵: Kcc の暗号化に間接的に適用して属性証明書に格納する処理形態について説明する。このグローバル共通鍵を利用する形態は、ユーザデバイスにおいてのみコンテンツ鍵: Kcc を取り出すことを可能とし、コンテンツの配信を実行するサービスプロバイダはコンテンツ鍵の取り出しを不可能とすることで、システムホルダの許可なくコンテンツが配布、利用されることを防止し、システムホルダ(SH)による管理されたコンテンツ配信を行なうことが可能となる。

【0196】具体的には、サービスプロバイダに対してコンテンツを提供するコンテンツクリエータの有するコンテンツ製作者鍵、コンテンツ配信を行なうサービスプロバイダの有するコンテンツ配信者鍵、そしてシステムホルダ(SH)とユーザデバイスで共有する鍵として生成されるグローバル共通鍵: Kg の各鍵を組み合わせた暗号化処理を行なった暗号化鍵データを属性証明書に格納する。

【0197】図27に、グローバル共通鍵: Kg をコンテンツ鍵: Kcc の暗号化に間接的に適用してコンテンツ鍵: Kcc の暗号化データを属性証明書に格納して配布する処理の詳細を説明する図を示す。

【0198】図27には、コンテンツ配信のプラットホームを構築、管理するシステムホルダ301、コンテンツ配信を実行するサービスプロバイダ(CD:コンテンツディストリビュータ)302、コンテンツを生成または管理し、サービスプロバイダ302に対して暗号化コンテンツを提供するコンテンツクリエータ303、サービスプロバイダ302からコンテンツを受領するエンドエンティティとしてのユーザデバイス304を示している。なお、ユーザデバイス304は、前述の(a)、(b)の例と同様、セキュリティチップを有し、セキュリティチップ内のメモリ領域にはサービスプロバイダ管理領域が生成されている。

【0199】図27の処理について説明する。まず、コンテンツクリエータ303は、配信対象となるコンテンツを暗号化するための鍵: Kcc を例えれば乱数により生成し、生成したコンテンツ鍵(共通鍵系): Kcc を用いて、(1)コンテンツを暗号化してサービスプロバイダ302に提供する。

【0200】さらに、システムホルダ301は、(2)コンテンツクリエータ303から、コンテンツクリエータ303の保有するコンテンツクリエータ鍵(共通鍵系): Kcc を受信し、(3)サービスプロバイダ(CD:コンテンツディストリビュータ)302からサービスプロバイダ302の保有するサービスプロバイダ鍵

(共通鍵系): Kcd を受信する。なお、これらの鍵は事前に受け渡しを行なってもよい。

【0201】システムホルダ301は、コンテンツクリエータ鍵: Kcc をサービスプロバイダ鍵: Kcd で暗号化し、さらに、この暗号化データをグローバル共通鍵: Kg で暗号化する。すなわち暗号化鍵データ: [Kg ([Kcd (Kcc)])] を生成し、(4)これをコンテンツクリエータ303に送付する。なお、[Kg ([Kcd (Kcc)])] は事前に受け渡しを行なってもよい。グローバル共通鍵: Kg は、システムホルダ301と、ユーザデバイス304が共有する鍵である。ユーザデバイス304には、(5)デバイス製造時、デバイス販売時まで、あるいは少なくともコンテンツの購入開始前までに、1以上のグローバル共通鍵: Kg1 ~ Kg n が格納され、これらはシステムホルダの管理の下に更新処理が実行される。更新処理については、後述する。

【0202】コンテンツクリエータ303は、コンテンツ鍵: Kcc をコンテンツクリエータ鍵: Kcc で暗号化したデータ: [Kcc (Kcc)] を生成し、(6)これをサービスプロバイダ302に対して送信するとともに、システムホルダ301から受信した、コンテンツクリエータ鍵: Kcc をサービスプロバイダ鍵: Kcd で暗号化し、さらに、この暗号化データをグローバル共通鍵: Kg で暗号化した暗号化鍵データ: [Kg ([Kcd (Kcc)])] をサービスプロバイダ302に対して送信する。なお、[Kg ([Kcd (Kcc)])] は事前に受け渡しを行なってもよい。

【0203】ユーザデバイス304がサービスプロバイダ302に対して(7)コンテンツ購入要求を行なうと、(8)サービスプロバイダは、要求コンテンツに対応する属性証明書を生成して、ユーザデバイス304に送信する。生成する属性証明書(AC)には、前述の暗号鍵データ: [Kg ([Kcd (Kcc)])]、すなわち、コンテンツクリエータ鍵: Kcc をサービスプロバイダ鍵: Kcd で暗号化し、さらに、この暗号化データをグローバル共通鍵: Kg で暗号化したデータ、および、コンテンツ鍵: Kcc をコンテンツクリエータ鍵: Kcc で暗号化したデータ: [Kcc (Kcc)] が格納される。その他、コンテンツの利用条件等のデータが格納され、サービスプロバイダ302の電子署名がなされてユーザデバイス304に送信される。ユーザデバイス304は、受信した属性証明書(AC)をメモリに格納する。

【0204】コンテンツの利用時には、ユーザデバイス304は、サービスプロバイダ302との間で(9)相互認証を行なった後、(10)先に受信済みの属性証明書(AC)をサービスプロバイダ302に送信する。相互認証処理は、ユーザデバイスのセキュリティチップとサービスプロバイダ間の相互認証処理として実行され

る。この相互認証処理は、先に説明した図16のTLS 1.0処理または、その他の方式、例えば公開鍵方式による相互認証処理として実行される。この相互認証処理においては、相互の公開鍵証明書の検証がなされ、必要に応じてルート認証局(CA)までの公開鍵証明書が連鎖的に検証される。この認証処理において、セキュリティチップと、サービスプロバイダはセッション鍵(Kses)を共有する。

【0205】属性証明書には、前述のコンテンツクリエータ鍵:Kccをサービスプロバイダ鍵:Kcdで暗号化し、さらに、この暗号化データをグローバル共通鍵:Kgで暗号化したデータ:[Kg([Kcd(Kcc)])]、および、コンテンツ鍵:Kcをコンテンツクリエータ鍵:Kccで暗号化したデータ:[Kcc(Kc)]が格納されている。

【0206】セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、(11)サービスプロバイダは、自己の所有するサービスプロバイダ鍵:Kcdを、相互認証時に生成したセッション鍵:Ksesで暗号化して、暗号化鍵データ[Kses(Kcd)]を生成し、これをユーザデバイスに送信する。

【0207】ユーザデバイス304のセキュリティチップ制御部は、(12)サービスプロバイダ302から受信した暗号化鍵データ[Kses(Kcd)]について、セッションキーを用いた復号化処理を実行してサービスプロバイダ鍵:Kcdを取得する。なお、サービスプロバイダ鍵:Kcdを事前にサービスプロバイダメモリ領域に保管しておいてもよい。

【0208】ユーザデバイス304のセキュリティチップ制御部は、次に、(13)属性証明書中のコンテンツクリエータ鍵:Kccをサービスプロバイダ鍵:Kcdで暗号化し、さらに、この暗号化データをグローバル共通鍵:Kgで暗号化したデータ:[Kg([Kcd(Kcc)])]について、まず、自己の所有するグローバル共通鍵:Kgで復号し、[Kcd(Kcc)]を取得する。さらに、(14)サービスプロバイダ302から受信した暗号化鍵データの復号により取得したサービスプロバイダ鍵:Kcdを適用した復号化処理により、コンテンツクリエータ鍵:Kccを取得する。

【0209】さらに、(15)ユーザデバイス304のセキュリティチップ制御部は、属性証明書中のコンテンツ鍵:Kcをコンテンツクリエータ鍵:Kccで暗号化したデータ:[Kcc(Kc)]を取り出して、前記処理によって取得したコンテンツクリエータ鍵:Kccを適用した復号化処理を実行してコンテンツ鍵:Kcを取

得する。

【0210】コンテンツ鍵:Kcの取得に成功すると、ユーザデバイス304のセキュリティチップ制御部は、ユーザデバイス制御部にコンテンツの復号準備が完了したことを通知する。

【0211】ユーザデバイス304は、サービスプロバイダ302から取得した暗号化コンテンツ((16)の処理)をセキュリティチップに送信し、セキュリティチップ内で暗号化コンテンツに対してコンテンツ鍵:Kcを適用した復号化処理を実行する。

【0212】なお、上述の各エンティティ間における鍵、暗号化鍵等のデータ送受信の前には、データ送受信を実行するエンティティ間で相互認証を実行し、認証成立を条件としたデータ送受信を行なうことが好ましく、また送受信データはセッションキーで暗号化し、署名を付与した構成とすることが好ましい。

【0213】このように、グローバル共通鍵は、ユーザデバイスとシステムホルダのみが所有し、その他のエンティティは保有することがなく、他のエンティティでは取得不可能な鍵として構成される。従って、サービスプロバイダにおいてもコンテンツ鍵の取得は不可能であり、システムホルダの許可のないコンテンツ鍵の流通、コンテンツの流通が防止可能となる。

【0214】グローバル共通鍵は、必要に応じて更新される。更新を実行するのは、システムホルダの管理下にあるサポートセンタである。サポートセンタとユーザデバイス間で実行されるグローバル共通鍵更新処理シーケンスを図28に示す。ユーザデバイスのセキュリティチップ内のメモリ領域には、2つのグローバル共通鍵Kg1, Kg2が格納されているものとする。これらのいずれかを使用して属性証明書内の鍵データの暗号化がなされ、復号化処理が実行される。あるいは例えばトリブルDESアルゴリズムを適用して2つの鍵を用いて属性証明書内の鍵データの暗号化を行ない、2つの鍵を用いた復号化処理を実行する構成としてもよい。

【0215】図28の処理シーケンスに示す各処理について説明する。図28は左からセキュリティチップ制御部、ユーザデバイス制御部、システムホルダの管理下にあるサポートセンタにおける処理を示している。

【0216】まず、ユーザデバイス制御部がグローバル共通鍵:Kg更新要求をセキュリティチップ制御部に送信すると、セキュリティチップ制御部は、システムホルダの管理下にあるサポートセンタに対してユーザデバイスを介して接続し、セキュリティチップとサポートセンタ間の相互認証処理を実行する。この相互認証処理は、先に説明した図16のTLS 1.0処理または、その他の方式、例えば公開鍵方式による相互認証処理として実行される。この相互認証処理においては、相互の公開鍵証明書の検証がなされ、必要に応じてルート認証局(CA)までの公開鍵証明書が連鎖的に検証される。この認

証処理において、セキュリティチップと、サポートセンタはセッション鍵（Kses）を共有する。

【0217】相互認証が成立すると、セキュリティチップの制御部は、サポートセンタに対してグローバル共通鍵：Kg更新要求を出力する。サポートセンタは、すでに生成済みの更新用グローバル共通鍵：Kg3、あるいは要求に応じて生成したグローバル共通鍵：Kg3を認証処理において生成したセッション鍵：Ksesで暗号化し、暗号化鍵データ：[Kses(Kg3)]をユーザデバイスのセキュリティチップに対して送信する。

【0218】セキュリティチップの制御部は、サポートセンタからセッションキーで暗号化されたグローバル共通鍵：Kg3、すなわち、[Kses(Kg3)]を受信すると、相互認証時に保有したセッションキーを用いて復号化処理を実行してグローバル共通鍵：Kg3を取得する。

【0219】グローバル共通鍵：Kg3の取得に成功すると、セキュリティチップ制御部は、グローバル共通鍵：Kg1を、取得したグローバル共通鍵：Kg3に置き換える。これにより、ユーザデバイスの保有するグローバル共通鍵は、Kg2、Kg3となる。ユーザデバイスの保有するグローバル共通鍵は、その順序関係も含めて意味があるため、[Kg1, Kg2]の順序関係も併せて[Kg2, Kg3]と修正する。グローバル共通鍵は、鍵データと共にユーザデバイス内で保持されている順序関係も合わせてデータを保持しているものとする。

【0220】図29は、ユーザデバイスとサポートセンタが直接データ送受信を行なうことなく、サービスプロバイダが仲介を行なってグローバル共通鍵の更新を実行する処理シーケンス例を示した図である。

【0221】図29の処理シーケンスに示す各処理について説明する。図29は左からセキュリティチップ制御部、ユーザデバイス制御部、サービスプロバイダ、システムホルダの管理下にあるサポートセンタにおける処理を示している。

【0222】サポートセンタでは、更新される新たなグローバル共通鍵：Kg3を事前生成し、グローバル共通鍵：Kg3をすでにユーザデバイスに配布済みのグローバル共通鍵：Kg2で暗号化してデータ：[Kg2(Kg3)]を生成し、これに、サポートセンタの秘密鍵：Kssで署名をしてサービスプロバイダに送付する。サービスプロバイダは、データ[Kg2(Kg3)]、Sig[Kss]を有する。なお、A、Sig[B]は、データAに鍵Bで署名を付加したデータ構成を示すものとする。

【0223】次に、ユーザデバイス制御部がグローバル共通鍵：Kg更新要求をセキュリティチップ制御部に送信すると、セキュリティチップ制御部は、サービスプロバイダに対してユーザデバイスを介して接続し、セキュリティチップとサービスプロバイダ間の相互認証処理を

実行する。この相互認証処理は、先に説明した図16のTLS1.0処理または、その他の方式、例えば公開鍵方式による相互認証処理として実行される。この相互認証処理においては、相互の公開鍵証明書の検証がなされ、必要に応じてルート認証局（CA）までの公開鍵証明書が連鎖的に検証される。この認証処理において、セキュリティチップと、サービスプロバイダはセッション鍵（Kses）を共有する。

【0224】相互認証が成立すると、セキュリティチップの制御部は、サービスプロバイダに対してグローバル共通鍵：Kg更新要求を出力する。サービスプロバイダはサポートセンタから受信済みのデータ[Kg2(Kg3)]、Sig[SuC]をユーザデバイスのセキュリティチップに対して送信する。

【0225】セキュリティチップの制御部は、サービスプロバイダから、サポートセンタからのデータ[Kg2(Kg3)]、Sig[SuC]の転送を受けると、署名検証処理を実行し、データ改竄のないことを確認した後、自己の所有するグローバル共通鍵：Kg2で暗号化されたグローバル共通鍵：Kg3、すなわち、[Kg2(Kg3)]に対して、グローバル共通鍵：Kg2を用いた復号化処理を実行してグローバル共通鍵：Kg3を取得する。なお、サポートセンタの署名検証にサポートセンタの公開鍵を適用する場合は、サポートセンタの公開鍵証明書をユーザデバイスに対してデータ[Kg2(Kg3)]、Sig[SuC]とともに送信するか、あるいはユーザデバイスに予め配布しておく。

【0226】グローバル共通鍵：Kg3の取得に成功すると、セキュリティチップ制御部は、メモリの鍵格納領域、例えば前述のデバイス管理領域内のグローバル共通鍵：Kg1書き込み領域にグローバル共通鍵：Kg3を上書きする。この更新処理により、ユーザデバイスの保有するグローバル共通鍵は、Kg2、Kg3の2つに更新される。

【0227】[デコーダを利用した復号化処理] 暗号化コンテンツ、あるいは暗号化コンテンツ鍵は、専用の復号化処理機能を持つデコーダに処理を実行させる構成とすると処理の高速化が可能となる。ただし、デコーダはセキュリティチップと独立したハード構成を持つため、40 デコーダの信頼性を確認した上でデコーダ内のコンテンツ鍵、コンテンツの復号化を行なうことが必要となる。以下、デコーダを用いた暗号化コンテンツ、あるいは暗号化コンテンツ鍵の復号化処理について図を参照して説明する。

【0228】図30にユーザデバイスにセキュリティチップと、デコーダを有する場合のコンテンツ鍵、コンテンツの復号化処理シーケンスを説明する図を示す。

【0229】ユーザデバイスは、セキュリティチップ210と、デコーダ280、ハードディスク、フラッシュメモリ等からなるメモリ部222と、上位ソフトウェア

によりセキュリティチップ210と、デコーダ280、メモリ部222に対してデータ入出力、各種処理実行命令を行なうユーザデバイス側制御部221がある。

【0230】コンテンツ復号化処理時のシーケンスについて説明する。まず、ユーザによる入力手段の操作により、コンテンツを指定したコンテンツ利用要求がユーザデバイス側制御部221に入力されると、ユーザデバイス側制御部221は、メモリ部222に格納された指定コンテンツに対応する属性証明書(AC)を検索する。検索により抽出された属性証明書(AC)はセキュリティチップ210に転送され、セキュリティチップ210内で、属性証明書(AC)の検証処理が実行される。

【0231】属性証明書(AC)検証処理に成功すると、セキュリティチップ210とデコーダ280間ににおいて相互認証およびセッション鍵の共有処理が実行される。相互認証が成立した後、セキュリティチップ210は、属性証明書(AC)から取り出した暗号化コンテンツ鍵を復号化した後、相互認証時にデコーダ280と共有したセッション鍵を用いてコンテンツ鍵を再暗号化してデコーダ280に送信する。暗号化コンテンツ鍵を受信したデコーダ280は、セッション鍵を適用して暗号化コンテンツ鍵の復号化を実行してコンテンツ鍵を取得する。

【0232】次に、ユーザデバイス側制御部221は、メモリ部222に格納された暗号化コンテンツを検索して取り出し、デコーダ280に送信する。デコーダ280は、入力された暗号化コンテンツを先に取得したコンテンツ鍵を適用して復号化処理を実行する。

【0233】上述したデコーダを適用した処理では、コンテンツ鍵はセキュリティチップ210内では使用されない。また、デコーダは、暗号化コンテンツを復号化して、アナログ出力として音声または映像データを外部出力する。なお、属性証明書(AC)には、認証するデコーダのIDや認証方式を記述してもよく、この場合、セキュリティチップ210は、相互認証時にデコーダが属性証明書(AC)に記述されたデコーダIDや認証方式に適合するか否かを判定して、適合する場合にのみコンテンツ鍵をデコーダに出力する。

【0234】デコーダを用いた処理シーケンスについて図31を用いて説明する。図31において、左からセキュリティチップ、上位ソフトウェア(ユーザデバイス側制御部)、デコーダの各処理を示している。

【0235】利用者による入力手段の操作により、コンテンツを指定したコンテンツ利用要求が上位ソフトウェア(ユーザデバイス側制御部)に入力されると、上位ソフトウェア(ユーザデバイス側制御部)は指定コンテンツに対応するアプリケーションIDを取得し、アプリケーションIDに基づいて、ハードディスク等のメモリに格納されたアプリケーションIDに対応する属性証明書(AC)を検索する。

【0236】検索により抽出された属性証明書(AC)は、属性証明書(AC)検証処理命令とともにセキュリティチップに転送され、セキュリティチップは、属性証明書(AC)の検証処理を実行し、属性証明書(AC)検証処理に成功すると、セキュリティチップは、属性証明書(AC)から暗号化コンテンツ鍵を取り出して、復号化処理を実行するとともに、上位ソフトウェア(ユーザデバイス側制御部)に応答メッセージを出力する。

【0237】次に、セキュリティチップとデコーダ間ににおいて、上位ソフトウェア(ユーザデバイス側制御部)を介して相互認証およびセッション鍵の共有処理が実行される。相互認証が成立した後、セキュリティチップは、属性証明書(AC)から取り出した暗号化コンテンツ鍵を復号化した後、相互認証時にデコーダと共有したセッション鍵を用いてコンテンツ鍵を再暗号化してデコーダに送信する。暗号化コンテンツ鍵を受信したデコーダは、セッション鍵を適用して暗号化コンテンツ鍵の復号化を実行してコンテンツ鍵を取得する。

【0238】次に、ユーザデバイス側制御部は、メモリに格納された暗号化コンテンツを検索して取り出し、デコーダに送信する。デコーダは、入力された暗号化コンテンツを先に取得したコンテンツ鍵を適用して復号化処理を実行する。

【0239】次に、デコーダを用いたコンテンツ復号化処理について、図32のフローを参照して説明する。

【0240】ステップS101において、利用者による入力手段の操作により、コンテンツを指定したコンテンツ利用要求が上位ソフトウェア(ユーザデバイス側制御部)に入力されると、ステップS102において、上位ソフトウェア(ユーザデバイス側制御部)は指定コンテンツに対応するアプリケーションIDを取得し、ステップS103において、アプリケーションIDに基づいて、ハードディスク等のメモリに格納されたアプリケーションIDに対応する属性証明書(AC)を検索する。検索により抽出された属性証明書(AC)は、ステップS104において、属性証明書(AC)検証処理命令とともにセキュリティチップに転送され、セキュリティチップは、ステップS105において、属性証明書(AC)の検証処理を実行し、属性証明書(AC)検証処理に成功すると、セキュリティチップは、属性証明書(AC)から暗号化コンテンツ鍵を取り出して、復号化処理を実行する。また、ステップS106において、上位ソフトウェア(ユーザデバイス側制御部)に応答メッセージを出力する。

【0241】属性証明書(AC)検証処理に成功しなかった場合は、その後の処理は中止される。検証成功の場合は、セキュリティチップとデコーダ間ににおいて、上位ソフトウェア(ユーザデバイス側制御部)を介して相互認証およびセッション鍵の共有処理が実行される。具体的には、ステップS108において、上位ソフトウェア

(ユーザデバイス側制御部)からセキュリティチップに第1認証コマンドが発行され、ステップS109においてセキュリティチップからの応答を上位ソフトウェア(ユーザデバイス側制御部)が受信し、さらに、ステップS110において、上位ソフトウェア(ユーザデバイス側制御部)からデコーダに第2認証コマンドが発行され、ステップS111においてデコーダからの応答を上位ソフトウェア(ユーザデバイス側制御部)が受信し、さらに、ステップS112において、上位ソフトウェア(ユーザデバイス側制御部)からセキュリティチップに第3認証コマンドが発行され、ステップS113においてセキュリティチップからの応答を上位ソフトウェア(ユーザデバイス側制御部)が受信する処理によって、セキュリティチップによるデコーダの認証処理が実行される。認証処理が失敗した場合(S114でNG)は、その後の処理は中止され、成功した場合は、ステップS115に進む。

【0242】ステップS115において、上位ソフトウェア(ユーザデバイス側制御部)からデコーダに第4認証コマンドが発行され、ステップS116においてデコーダからの応答を上位ソフトウェア(ユーザデバイス側制御部)が受信する。この処理によって、デコーダによるセキュリティチップの認証の成否が判定される。認証処理が失敗の場合(S117でNG)は、その後の処理は中止され、成功した場合は、ステップS118に進む。

【0243】ステップS118において、セキュリティチップは、属性証明書(A C)から取り出した暗号化コンテンツ鍵を復号化した後、相互認証時にデコーダと共にセッション鍵を用いてコンテンツ鍵を再暗号化(S118)して、上位ソフトウェア(ユーザデバイス側制御部)に送信(S119)する。上位ソフトウェア(ユーザデバイス側制御部)は、受信した暗号化コンテンツ鍵をデコーダに送信(S120)する。

【0244】暗号化コンテンツ鍵を受信したデコーダは、セッション鍵を適用して暗号化コンテンツ鍵の復号化を実行してコンテンツ鍵を取得(S121)する。上位ソフトウェア(ユーザデバイス側制御部)は、メモリに格納された暗号化コンテンツを検索(S122)して取り出し、デコーダに送信(S123)する。デコーダは、入力された暗号化コンテンツを先に取得したコンテンツ鍵を適用して復号化処理を実行(S124)する。

【0245】このように、デコーダを用いた復号化処理においては、セキュリティチップとデコーダ間の相互認証が実行されて、相互認証の成立を条件として、セッション鍵で暗号化したコンテンツ鍵がデコーダに出力する構成としたので、信頼される機器においてのみ復号が実行され、正当なコンテンツ利用を確保することができる。

【0246】[コンテンツの利用制限] 先に説明したよ

うに、コンテンツの利用制限情報を格納したコンテンツ対応の属性証明書中の属性情報フィールドに格納されるコンテンツ利用条件関連情報には、サービスプロバイダの提供するコンテンツの利用制限回数、利用期限等の様々な利用条件が含まれる。すなわち、以下の情報である。

条件：オンライン利用コンテンツか、オフライン利用コンテンツか、さらに、買い切りコンテンツ、期間制限コンテンツ、オンライン回数制限コンテンツ、オフライン回数制限コンテンツのいずれであるかを示す情報  
有効期限：期間制限の場合の有効期限情報  
利用制限回数：回数制限の場合の利用可能回数

【0247】コンテンツを買い切りし、買い切り以後のコンテンツ利用をフリーとするコンテンツに対応する属性証明書は、上記条件が買い切りとして設定される。利用期間を設定したコンテンツに対応する属性証明書は、上記条件が期間制限として設定され、有効期限が設定される。利用回数制限を設定したコンテンツに対応する属性証明書は、上記条件が回数制限として設定され、利用制限回数に設定値(回数値)が設定される。なお、回数制限処理の場合には、ユーザデバイス内で利用可能回数を管理してコンテンツ利用を実行するオフライン回数制限と、サービスプロバイダにおいて回数検証をした後、属性証明書に記録された設定回数以内のコンテンツ利用を許可するオンライン回数制限がある。また期間制限と回数制限の両制限を伴うコンビネーション制限態様もある。ユーザデバイスでは、属性証明書に記録されたこれらの態様に従ってコンテンツが利用される。これらの具体的な処理態様について、以下、説明する。

【0248】ユーザデバイスにおいてコンテンツを利用するためには、利用対象となるコンテンツに対応する属性証明書中から暗号化コンテンツ鍵を取り出して復号化処理を実行してコンテンツ鍵:Kcを取得することが必要となる。このコンテンツ鍵の取得処理には、デバイスのセキュリティチップ内で実行するオフライン処理、サービスプロバイダに属性証明書を送付して復号を依頼するオンライン処理があることは先に述べた通りである。属性証明書に記載されたコンテンツの利用条件に従ったコンテンツ利用処理においても、利用条件をユーザデバイス内で確認するオフライン処理、サービスプロバイダでの確認を必要とするオンライン処理がある。これらのどちらを適用するかは、属性証明書の属性情報フィールドの記載に従って決定する。

【0249】図33にコンテンツ利用時におけるユーザデバイスで実行される属性証明書(A C)の利用処理フローを示す。処理フローの各ステップについて説明する。

【0250】ユーザデバイスは、利用対象コンテンツに対応する属性証明書をアプリケーションID(コンテンツ識別情報)に基づいて選択すると、まず、属性証明書

のフォーマット確認処理を実行(S201)する。属性証明書に必要事項が記録され、証明書の有効期限が有効であるか等である。フォーマット確認処理が済むと、ステップS202において署名検証が実行される。先にも説明したように属性証明書には、属性証明書発行者(例えばサービスプロバイダ)の電子署名が付加されており、ユーザデバイスは、属性証明書発行者の公開鍵証明書から公開鍵を取り出して署名検証処理(図20参照)を行なう。なお、この際使用する公開鍵証明書の検証、連鎖的公開鍵証明書の検証処理も必要に応じて実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【0251】ステップS202の署名検証処理過程において、検証が成立し、属性証明書に改竄がないと判定された場合はステップS203に進む。一方、ステップS202の署名検証処理過程において、検証が非成立となり、属性証明書に改竄ありと判定された場合は、ステップS205に進み、その属性証明書を適用した処理は実行されず、以降の処理、すなわちコンテンツ利用処理が中止される。

【0252】属性証明書に改竄がないと判定され、ステップS203に進むと、属性証明書内の属性情報フィールド内のコンテンツ利用条件情報を取得する。すなわち、オンライン利用コンテンツか、オフライン利用コンテンツか、さらに、買い切りコンテンツ、期間制限コンテンツ、オンライン回数制限コンテンツ、オフライン回数制限コンテンツのいずれであるかである。この条件に従って、ステップS204のオンライン処理であるか、オフラインである場合は、ステップS206において買い切りか、回数制限であるかが判定される。

【0253】ステップS204において、オンライン利用であると判定されると、先に図26を用いて説明したと同様、属性証明書をサービスプロバイダに送付して属性証明書内の利用制限情報の検証が実行される。オンライン処理の場合は、期間制限、または回数制限のいずれかであり、サービスプロバイダはこれらのコンテンツ利用条件情報を属性証明書から取得して利用制限内のコンテンツ利用請求であれば、コンテンツ鍵の取得を可能とする処理を行なう。利用制限を超えたコンテンツ利用請求であれば、コンテンツ鍵の取得を可能とする処理を実行せず、コンテンツ利用不可であるメッセージをユーザデバイスに送信する。

【0254】また、ステップS204において、オフライン利用であると判定され、ステップS206で買い切りコンテンツであると判定された場合には、属性証明書には、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたSP対応ストレージ秘密鍵に対応するサービスプロバイダ(SP)対応ストレージ公開鍵:SC, St o p u b, SP, Kで暗号化されたコンテンツ鍵データ:[SC, St o p u b, S

P, K(Kc)]が格納されており、ユーザデバイスでは、サービスプロバイダ管理領域に格納されたSP対応ストレージ秘密鍵SC, St o p r i, SP, Kを用いて復号化処理を実行してコンテンツ鍵:Kcを取得して、コンテンツの復号によりコンテンツを利用する。

【0255】さらに、ステップS204において、オンライン利用であると判定され、ステップS206で回数制限のコンテンツであると判定された場合には、ユーザデバイス内で、属性証明書の設定条件に基づいて回数管理を実行して、コンテンツ利用の可否判定を実行した後、利用可であるとの判定結果の取得を条件として、属性証明書内に格納された暗号化コンテンツ鍵の復号化処理を実行し、かつ、デバイス内で管理するコンテンツ利用回数管理データの更新処理等を実行する。このためにデバイス内にコンテンツ利用回数の管理データを持つことが必要となる。

【0256】ステップS207の利用回数管理データのインポート処理は、コンテンツ利用回数の管理データ生成処理である。なお、利用回数管理データのインポート処理は、属性証明書に基づいて実行される。コンテンツ利用回数の管理態様には、コンテンツ利用可能回数をユーザデバイス内のセキュリティチップで管理する態様と、回数管理ファイルをセキュリティチップ外の外部メモリ(例えばハードディスク)に格納管理し、管理データのハッシュ値のみをセキュリティチップ内のメモリに格納する2つの態様がある。これらの詳細については後述する。ステップS208の属性証明書適用完了メッセージ生成ステップは、上述のS207の利用回数管理データのインポート処理が完了したことをセキュリティチップからセキュリティチップ外のユーザデバイスに通知する処理である。

【0257】以下、属性証明書(AC)に記載されたコンテンツ利用条件を以下の4態様に区別して、順次、説明する。

- (A) オンライン-利用期間制限コンテンツ
- (B) オンライン-利用回数制限コンテンツ
- (C) オフライン-買い切りコンテンツ
- (D) オフライン-利用回数制限コンテンツ

【0258】(A) オンライン-利用期間制限コンテン

40 ツまず、属性証明書に記録されたコンテンツ利用条件がオンライン処理であり、利用期間が制限されたコンテンツである場合の属性証明書の取得から、コンテンツ取得までの処理を図34のシーケンス図に従って説明する。

【0259】図34に示す処理シーケンスは、すでにサービスプロバイダから暗号化コンテンツを受領済みであり、また、コンテンツに対応する利用条件、暗号化コンテンツ鍵を格納した属性証明書を受領済みであるユーザデバイスにおける処理を示しており、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制

御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。

【0260】図34では、最上段（a）は、属性証明書がセキュリティチップの内部メモリに格納されている場合における属性証明書からのサービスプロバイダID取得処理、（b）は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダID取得処理を示し、これら（a）、（b）は属性証明書の格納位置に応じて選択的に実行する。（c）の相互認証処理、（d）のコンテンツ取得処理は共通に実行される。

【0261】まず、（a）の処理から説明する。（a1）ユーザデバイス制御部は、利用対象コンテンツに対応する属性証明書の検索をセキュリティチップ制御部に要求する。（a2）セキュリティチップ制御部は、チップのメモリに格納済みの属性証明書のリストをユーザデバイス制御部に出力し、（a3）ユーザデバイスでは付属のブラウザによりリストを表示する。（a4）ユーザは表示されたリストから利用予定コンテンツに対応する属性証明書（AC）を指定し、読み出し命令をセキュリティチップ制御部に送信する。（a5）セキュリティチップ制御部は、指定された属性証明書を内部メモリから読み出してユーザデバイス制御部に出力し、（a6）ユーザデバイスでは付属のブラウザにより属性証明書を表示し、属性証明書格納データ中のサービスプロバイダ識別子（SP-ID）を取得する。

【0262】属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合は、（b）の処理となる。（b1）ユーザデバイス制御部は、利用対象コンテンツに対応する属性証明書の検索を実行し、（b2）ユーザデバイスでは付属のブラウザにより表示されたACリストから利用予定コンテンツに対応する属性証明書（AC）を指定し、（b3）読み出して属性証明書を表示し、（b4）属性証明書格納データ中のサービスプロバイダ識別子（SP-ID）を取得する。

【0263】上記（a）、（b）のいずれかの処理によって取得されたサービスプロバイダ識別子（SP-ID）は、サービスプロバイダ管理領域から、相互認証に必要な情報を取得するために用いられる。前述したように、サービスプロバイダ管理領域へのアクセスにはサービスプロバイダ毎に設定されたパスワード入力が必要であり、ユーザは、属性証明書から取得したサービスプロバイダ識別子（SP-ID）に対応するパスワード入力により、サービスプロバイダ管理領域へのアクセスを実行し、図34の（c1）に示すセキュリティチップとサービスプロバイダ間の相互認証処理を実行する。

【0264】この相互認証処理は、先に説明した図16のTLS1.0処理または、その他の方式、例えば公開

鍵方式による相互認証処理として実行される。この相互認証処理においては、相互の公開鍵証明書の検証がなされ、必要に応じてルート認証局（CA）までの公開鍵証明書が連鎖的に検証される。この認証処理において、セキュリティチップと、サポートセンタはセッション鍵（Kses）を共有する。相互認証が成立すると、次に、図34（d）に示す処理、すなわちコンテンツ取得処理を実行する。

【0265】（d1）ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報（コンテンツ利用条件）を確認し、属性証明書を適用したコンテンツ利用要求をセキュリティチップに対して出力する。この例における属性証明書に記録されたコンテンツ利用条件は、オンライン期間制限である。

【0266】（d2）セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書（AC）適用要求を受信すると、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図20の処理フローと同様のシーケンスに従って実行される。

【0267】さらに、必要に応じてセキュリティチップの制御部は、属性証明書（AC）内のAC保持者の公開鍵証明書情報を従ってリンクする公開鍵証明書を取得して、公開鍵証明書の検証を行なうことが好ましい。例えば属性証明書（AC）の発行者の信頼度が不確かである場合には、属性証明書（AC）の発行者の公開鍵証明書の検証を行なうことによって、認証局の公開鍵証明書を正当に有しているか否かの判定が可能となる。なお、公開鍵証明書が前述したように階層構成をなしている場合は、経路を上位に辿って連鎖的な検証を行ない、ルート認証局（CA）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【0268】（d3）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対して属性証明書を送付する。属性証明書には、利用条件としてオンライン期間制限コンテンツであることが記録され、また有効期限データが格納されている。さらに、サービスプロバイダの保有する秘密鍵：SP、Sto、Kで暗号化されたコンテンツ鍵のデータ、すなわち、[SP、Sto、K（Kc）]が格納されている。

【0269】（d4）セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、属性証明書に格納された利

用条件データ、有効期限データを確認する。属性証明書に記録されている利用条件としての有効期限内のコンテンツ利用要求であると判定されると、属性証明書中に格納されたコンテンツの復号に適用するコンテンツ鍵：Kcの暗号化データ：[S P. S t o. K (Kc)]の復号を実行する。

【0270】サービスプロバイダは、自己の所有する秘密鍵：S P. S t o. Kを用いて、属性証明書に格納された暗号化コンテンツ鍵：[S P. S t o. K (Kc)]の復号化処理を実行し、コンテンツ鍵：Kcを取り出す。さらに、取り出したコンテンツ鍵：Kcを先の相互認証処理において生成したセッションキー（Kses）で暗号化して、ユーザデバイスのセキュリティチップに対して送信する。

【0271】(d 5) セキュリティチップの制御部は、サービスプロバイダからセッションキーで暗号化されたコンテンツ鍵、すなわち、[Kses (Kc)]を受信すると、相互認証時に保有したセッションキーを用いて復号化処理を実行してコンテンツ鍵：Kcを取得する。コンテンツ鍵：Kcの取得に成功すると、セキュリティチップ制御部は、ユーザデバイス制御部にコンテンツの復号準備が完了したことを通知する。

【0272】(d 6) 次にユーザデバイス制御部は、取得したコンテンツ鍵を適用して復号すべき暗号化コンテンツ〔Kc (Content)〕をユーザデバイス内のメモリ（例えばハードディスク）、あるいはセキュリティチップ制御部を介してセキュリティチップ内のメモリから取得する。さらに、取得した暗号化コンテンツをセキュリティチップに送信し、(d 7) セキュリティチップ内で暗号化コンテンツに対してコンテンツ鍵：Kcを適用した復号化処理を実行し、復号化処理結果として得られるコンテンツをユーザデバイス制御部に出力し、

(d 8) ユーザデバイスは、コンテンツを取得する。これらの処理が終了すると、(d 9) セキュリティチップの制御部は、復号化処理によって取得したコンテンツ鍵：Kc、およびコンテンツ（Content）を破棄する。

【0273】これらの処理によって、サービスプロバイダによる属性証明書（AC）に基づく利用期間の確認処理が行われ、制限された利用期間内である場合にのみ、コンテンツ鍵：Kcがセキュリティチップにおいて復号可能な状態で再暗号化されて送付され、セキュリティチップにおいてコンテンツ鍵が取得され、取得したコンテンツ鍵によるコンテンツの復号が実行されてユーザデバイスにおいてコンテンツ利用が可能となる。

【0274】なお、サービスプロバイダからユーザデバイスに対するコンテンツ配信あるいは属性証明書（AC：Attribute Certificate）の配信形態としては、ユーザ側からサービスプロバイダに対する要求に基づいて実行される形態と、ユーザの要求の有無に関係なく例え

ばサブスクリーバ契約を結んでいるユーザに対して、サービスプロバイダから一方的に送信するいわゆるプッシュ型の形態（プッシュ型モデル）のいずれの形態も可能である。プッシュ型モデルにおいては、サービスプロバイダが予め目標ユーザ向けの属性証明書（AC）を作成して配信することになる。

【0275】(B) オンライン-利用回数制限コンテンツ

次に、属性証明書に記録されたコンテンツ利用条件がオンライン処理であり、利用回数が制限されたコンテンツである場合の属性証明書の取得から、コンテンツ取得までの処理を図35のシーケンス図に従って説明する。

【0276】図35に示す処理シーケンスは、先に説明した図34の処理シーケンスと同様、すでにサービスプロバイダから暗号化コンテンツを受領済みであり、また、コンテンツに対応する利用条件、暗号化コンテンツ鍵を格納した属性証明書を受領済みであるユーザデバイスにおける処理を示しており、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。

【0277】図35に示す処理中、最上段（a）は、属性証明書がセキュリティチップの内部メモリに格納されている場合における属性証明書からのサービスプロバイダID取得処理、(b)は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダID取得処理を示し、これら(a)、(b)は属性証明書の格納位置に応じて選択的に実行する。(a)、(b)の各処理と、(c)の相互認証処理は、図34を参照して説明したオンライン期間制限の場合の処理と同様であるので説明を省略する。(c)の相互認証が成立すると、次に、図35(d)に示す処理、すなわちコンテンツ取得処理を実行する。

【0278】(d 1) ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報（コンテンツ利用条件）を確認し、属性証明書を適用したコンテンツ利用要求をセキュリティチップに対して出力する。この例における属性証明書に記録されたコンテンツ利用条件は、オンライン回数制限である。

【0279】(d 2) セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書（AC）適用要求を受信すると、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図20の処理フローと同様のシーケンスに従って実行される。この検証処理において、セキュリティチップの制御部は、属性証明書（AC）内のAC保持者の公開鍵証明書情報を従ってリンク

する公開鍵証明書から、上位に辿って連鎖的な検証を行ない、ルート認証局（CA）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【0280】(d3) 属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対して属性証明書を送付する。属性証明書には、利用条件としてオンライン回数制限コンテンツであることが記録され、また利用制限回数が格納されている。さらに、サービスプロバイダの保有する秘密鍵：S P. S t o. Kで暗号化されたコンテンツ鍵のデータ、すなわち、[S P. S t o. K (K c)]が格納されている。

【0281】(d4) セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、属性証明書に格納された利用条件データ、利用制限回数を確認する。利用可能回数は、サービスプロバイダ内のデータベースに格納されており、サービスプロバイダでは、データベース内の管理データを参照して属性証明書に記録された回数制限内のコンテンツ利用であるか否かを判定する。

【0282】属性証明書に記録された回数制限内のコンテンツ利用であると判定されると、属性証明書中に格納されたコンテンツの復号に適用するコンテンツ鍵：K c の暗号化データ：[S P. S t o. K (K c)]の復号を実行する。サービスプロバイダは、自己の所有する秘密鍵：S P. S t o. Kを用いて、属性証明書に格納された暗号化コンテンツ鍵：[S P. S t o. K (K c)]の復号化処理を実行し、コンテンツ鍵：K cを取り出す。

【0283】さらに、サービスプロバイダは、データベース内のコンテンツ利用回数管理データを更新し、利用対象コンテンツの対応する利用可能回数を1デクリメントする処理を行なう。さらに、サービスプロバイダでは、取り出したコンテンツ鍵：K cを先の相互認証処理において生成したセッションキー（K s e s）で暗号化して、ユーザデバイスのセキュリティチップに対して送信する。

【0284】(d5) セキュリティチップの制御部は、サービスプロバイダからセッションキーで暗号化されたコンテンツ鍵、すなわち、[K s e s (K c)]を受信すると、相互認証時に保有したセッションキーを用いて復号化処理を実行してコンテンツ鍵：K cを取得する。コンテンツ鍵：K cの取得に成功すると、セキュリティチップ制御部は、ユーザデバイス制御部にコンテンツの復号準備が完了したことを通知する。

【0285】(d6) 次にユーザデバイス制御部は、取得したコンテンツ鍵を適用して復号すべき暗号化コンテンツ[K c (Content)]をユーザデバイス内のメモリ（例えばハードディスク）、あるいはセキュリティチップ制御部を介してセキュリティチップ内のメモリから取得する。さらに、取得した暗号化コンテンツをセキュリティチップに送信し、(d7) セキュリティチップ内で暗号化コンテンツに対するコンテンツ鍵：K cを適用した復号化処理を実行し、復号化処理結果として得られるコンテンツをユーザデバイス制御部に出力し、(d8) ユーザデバイスは、コンテンツを取得する。これらの処理が終了すると、(d9) セキュリティチップの制御部は、復号化処理によって取得したコンテンツ鍵：K c、およびコンテンツ（Content）を破棄する。

【0286】これらの処理によって、サービスプロバイダによる属性証明書（AC）に基づくコンテンツ利用回数の確認処理が行われ、制限された利用回数内である場合にのみ、コンテンツ鍵：K cがセキュリティチップにおいて復号可能な状態で再暗号化されて送付され、セキュリティチップにおいてコンテンツ鍵が取得され、取得したコンテンツ鍵によるコンテンツの復号が実行されてユーザデバイスにおいてコンテンツ利用が可能となる。

【0287】なお、サービスプロバイダからユーザデバイスに対するコンテンツ配信あるいは属性証明書（AC：Attribute Certificate）の配信形態としては、ユーザ側からサービスプロバイダに対する要求に基づいて実行される形態と、ユーザの要求の有無に関係なく例えばサブスクリーパ契約を結んでいるユーザに対して、サービスプロバイダから一方的に送信するいわゆるプッシュ型の形態（プッシュ型モデル）のいずれの形態も可能である。プッシュ型モデルにおいては、サービスプロバイダが予め目標ユーザ向けの属性証明書（AC）を作成して配信することになる。

【0288】(C) オフライン一買い切りコンテンツ次に、属性証明書に記録されたコンテンツ利用条件がオフライン処理であり、買い切りコンテンツである場合の属性証明書の取得から、コンテンツ取得までの処理を図36のシーケンス図に従って説明する。

【0289】図36に示す処理シーケンスは、先に説明した図34、図35の処理シーケンスと同様、すでにサービスプロバイダから暗号化コンテンツを受領済みであり、また、コンテンツに対応する利用条件、暗号化コンテンツ鍵を格納した属性証明書を受領済みであるユーザデバイスにおける処理を示しており、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。

【0290】図36に示す処理中、最上段（a）は、属性証明書がセキュリティチップの内部メモリに格納され

ている場合における属性証明書からのサービスプロバイダID取得処理、(b)は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダID取得処理を示し、これら(a)、(b)は属性証明書の格納位置に応じて選択的に実行する。(a)、(b)の各処理は、図34を参照して説明したオンライン期間制限の場合の処理と同様であるので説明を省略する。(a)、(b)のいずれかの処理によって、サービスプロバイダIDが取得されると、次に、図36(c)に示す処理、すなわちコンテンツ取得処理を実行する。

【0291】(c1)ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報(コンテンツ利用条件)を確認し、属性証明書を適用したコンテンツ利用要求をセキュリティチップに対して出力する。この例における属性証明書に記録されたコンテンツ利用条件は、オフライン買い切りである。

【0292】(c2)セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書(AC)適用要求を受信すると、属性証明書の検証処理を実行する。検証処理には、権限情報(コンテンツ利用条件)の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図20の処理フローと同様のシーケンスに従って実行される。この検証処理において、セキュリティチップの制御部は、属性証明書(AC)内のAC保持者の公開鍵証明書情報に従ってリンクする公開鍵証明書から、上位に辿って連鎖的な検証を行ない、ルート認証局(CA)の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【0293】(c3)属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップ制御部は、属性証明書内に格納された暗号化コンテンツ鍵:[SC. Stopub. SP. K(Kc)]を取り出して、サービスプロバイダ管理領域に格納されたSP対応ストレージ秘密鍵:SC. Stopri. SP. Kを適用して復号化処理を実行し、コンテンツ鍵:Kcを取得する。コンテンツ鍵:Kcの取得に成功すると、セキュリティチップ制御部は、ユーザデバイス制御部にコンテンツの復号準備が完了したことを通知する。

【0294】(c4)次にユーザデバイス制御部は、取得したコンテンツ鍵を適用して復号すべき暗号化コンテンツ[Kc(Content)]をユーザデバイス内のメモリ(例えばハードディスク)、あるいはセキュリティチップ制御部を介してセキュリティチップ内のメモリから取得する。さらに、取得した暗号化コンテンツをセキュリティチップに送信し、(c5)セキュリティチップ内で暗号化コンテンツに対してコンテンツ鍵:Kcを適用した復号化処理を実行し、復号化処理結果として得

られるコンテンツをユーザデバイス制御部に出力し、(c6)ユーザデバイスは、コンテンツを取得する。これらの処理が終了すると、(c7)セキュリティチップの制御部は、復号化処理によって取得したコンテンツ鍵:Kc、およびコンテンツ(Content)を破棄する。

【0295】これらの処理によって、属性証明書(AC)に基づく買い切りコンテンツであるとの確認処理が行われ、コンテンツ鍵:Kcがセキュリティチップにおいて復号され、コンテンツ鍵が取得され、取得したコンテンツ鍵によるコンテンツの復号が実行されてユーザデバイスにおいてコンテンツ利用が可能となる。

【0296】なお、上記構成例では、公開鍵暗号方式を適用し、コンテンツ鍵の暗号化にSP対応ストレージ公開鍵:SC. Stopub. SP. Kを用い、コンテンツ鍵の復号にSP対応ストレージ秘密鍵:SC. Stopri. SP. Kを用いた構成としたが、共通鍵方式を適用することも可能であり、共通鍵方式を適用する場合は、コンテンツ鍵の暗号化、復号化の双方の処理にSP対応ストレージ鍵(共通鍵):SC. Stop. SP. Kを用いる。この場合、SP対応ストレージ鍵(共通鍵):SC. Stop. SP. Kは、セキュリティチップのメモリの対応するサービスプロバイダのサービスプロバイダ管理領域に格納される。

【0297】なお、サービスプロバイダからユーザデバイスに対するコンテンツ配信あるいは属性証明書(AC:Attribute Certificate)の配信形態としては、ユーザ側からサービスプロバイダに対する要求に基づいて実行される形態と、ユーザの要求の有無に関係なく例えばサブスクライバ契約を結んでいるユーザに対して、サービスプロバイダから一方的に送信するいわゆるプッシュ型の形態(プッシュ型モデル)のいずれの形態も可能である。プッシュ型モデルにおいては、サービスプロバイダが予め目標ユーザ向けの属性証明書(AC)を作成して配信することになる。

【0298】(D) オフライン-利用回数制限コンテンツ  
次に、属性証明書に記録されたコンテンツ利用条件がオフライン処理であり、利用回数の制限されたコンテンツである場合の属性証明書の取得から、コンテンツ取得までの処理について説明する。属性証明書の利用条件がオフライン利用で、回数制限のあるコンテンツである場合、ユーザデバイス内で、属性証明書の設定条件に基づいて回数管理を実行するために、デバイス内にコンテンツ利用回数の管理データを持つことが必要となる。コンテンツ利用回数の管理データの保有処理が利用回数管理データのインポート処理である。  
【0299】(D-1) インポート処理  
まず、利用回数管理データのインポート処理について説明する。コンテンツ利用回数の管理態様には、コンテン

ツ利用可能回数をユーザデバイス内のセキュリティチップで管理する様と、回数管理ファイルをセキュリティチップ外の外部メモリ（例えばハードディスク）に格納管理し、管理データのハッシュ値のみをセキュリティチップ内のメモリに格納する2つの様がある。

【0300】最初に図37を参照して、コンテンツ利用可能回数をユーザデバイス内のセキュリティチップで管理する様とした場合の利用回数管理データのインポート処理シーケンスを説明する。左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。図37の処理シーケンスは、すでにコンテンツ購入処理に伴うセキュリティチップと、サービスプロバイダ間の相互認証が成立し、サービスプロバイダからセキュリティチップに対する、購入コンテンツに対応する属性証明書の発行処理以降の処理を示している。ここで、サービスプロバイダの発行する属性証明書は、コンテンツ利用条件として、オンライン利用での利用回数制限コンテンツであることが記録され、コンテンツ利用制限回数が記録されている。

【0301】（1）属性証明書がサービスプロバイダから発行され、送信されると、（2）セキュリティチップの制御部は、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図20の処理フローと同様のシーケンスに従って実行される。この検証処理において、セキュリティチップの制御部は、属性証明書（AC）内のAC保持者の公開鍵証明書情報を従ってリンクする公開鍵証明書から、上位に辿って連鎖的な検証を行ない、ルート認証局（CA）の発行した公開鍵証明書の検証まで実行することが好みしい。なお、この連鎖検証が必須の場合もある。

【0302】（3）セキュリティチップの制御部は、属性証明書に記録されたコンテンツ利用条件がオンライン利用回数制限コンテンツであると判定すると、属性証明書からコンテンツ識別子に対応するアプリケーションID、属性証明書（AC）シリアル番号、コンテンツ利用制限回数の各データを取得する。さらに、コンテンツの購入処理時にユーザにより入力されたユーザID、サービスプロバイダIDの各データをユーザデバイス制御部を介して取得し、これらの取得したアプリケーションID、属性証明書（AC）シリアル番号、ユーザIDの各データに対応するコンテンツ利用回数管理データが、セキュリティチップ内のメモリのサービスプロバイダ管理領域に登録済みであるか否かを検証する。なお、ユーザがユーザデバイスにログインしている場合には、ユーザID等は保持されているので、ユーザID、サービスプロバイダIDはユーザが入力する代わりにユーザデバイスが送信してもよい。

【0303】セキュリティチップのメモリには、前述したように、登録されたサービスプロバイダ毎にサービスプロバイダ管理領域が設定され、その管理領域内にコンテンツ利用回数管理データが登録されることになる。図38にセキュリティチップ内のメモリのサービスプロバイダ管理領域内に設定されるコンテンツ利用回数管理データの構成例を示す。

【0304】図38に示すように、サービスプロバイダ管理領域には、サービスプロバイダID、ユーザID毎に、コンテンツ識別子としてのアプリケーションID（App. ID #n）、対応する属性証明書（AC）の識別子であるACシリアル（AC Serial #n）、さらに残りの利用可能回数データ（Count #n）が対応付けられて格納される。同一のコンテンツであっても利用ユーザ毎に異なる属性証明書に基づく利用回数カウントを可能としたデータ構成となっている。

【0305】図37に戻って利用回数管理データのインポート処理のシーケンスについて説明を続ける。（3）セキュリティチップの制御部は、属性証明書から取得したコンテンツ識別子に対応するアプリケーションID、属性証明書（AC）シリアル番号、コンテンツ利用制限回数の各データ、ユーザにより入力されたユーザID、サービスプロバイダIDの各データに対応するコンテンツ利用回数管理データが、セキュリティチップ内のメモリのサービスプロバイダ管理領域に登録済みであるか否かを検証し、コンテンツ利用回数管理データが登録されていないことを確認すると、（4）コンテンツ利用回数管理データをサービスプロバイダ管理領域に追加登録し、（5）追加登録の終了後、属性証明書受信メッセージを生成して、サービスプロバイダに送信する。

【0306】図37の例では、サービスプロバイダから受領した属性証明書（AC）は、  
アプリケーションID：0001  
属性証明書（AC）シリアル：1345  
コンテンツ利用制限回数：5  
の各データが記録され、ユーザ入力データは、  
ユーザID：6737  
サービスプロバイダID：5678  
である。

【0307】セキュリティチップの制御部は、これらのデータに対応するコンテンツ利用回数管理データがメモリ内の対応するサービスプロバイダ管理領域にあるか否かを検証する。図37に示すSP管理領域データ（更新前）のデータ中には、サービスプロバイダID：5678、ユーザID：6737に対応するコンテンツ利用回数管理データとして、アプリケーションID：0001、属性証明書（AC）シリアル：1345に対応するデータは存在しない。

【0308】従って、今回サービスプロバイダから受領した属性証明書に対応するコンテンツ利用回数管理データ

タをサービスプロバイダ I D : 5678、ユーザ I D : 6737 に対応するコンテンツ利用回数管理データとして、新たに追加する処理を行なう。その結果、図の下段に示す S P 管理領域データ（更新後）のデータ中に、アプリケーション I D : 0001、属性証明書（A C）シリアル：1345 の回数管理データが追加され、利用可能回数として、受領した属性証明書に記録されたコンテンツ利用制限回数：5 が設定される。

【0309】コンテンツの利用時には、このコンテンツ利用回数管理データが参照され、利用毎に利用可能回数を 1 デクリメントして、5 → 4 → 3 → 2 → 1 → 0 とするデータ更新が実行され、利用可能回数が 0 となった以後のコンテンツ利用が拒否され、属性証明書に記録された利用制限回数内のコンテンツ利用が可能となる。このコンテンツ利用処理については、後述する。

【0310】なお、サービスプロバイダから受領した属性証明書のアプリケーション I D、属性証明書（A C）シリアルと同一のデータがすでに、対応するサービスプロバイダ I D、ユーザ I D のサービスプロバイダ管理領域内のコンテンツ利用回数管理データとして登録済みである場合には、重複した属性証明書の発行であると判定し、その属性証明書に基づくコンテンツ利用回数管理データの追加登録は実行しない。

【0311】また、サービスプロバイダから受領した属性証明書のアプリケーション I D と同一であるが、属性証明書（A C）シリアルが異なるデータがすでに、対応するサービスプロバイダ I D、ユーザ I D のサービスプロバイダ管理領域内のコンテンツ利用回数管理データとして登録済みである場合には、異なる属性証明書に基づく同一コンテンツの新たな利用を可能とする属性証明書であると判定し、その属性証明書に基づくコンテンツ利用回数管理データの追加登録を実行する。

【0312】すなわち、同一のサービスプロバイダ I D、同一ユーザ I D のサービスプロバイダ管理領域内のコンテンツ利用回数管理データとして、すでに、例えばアプリケーション I D : 0001、A C シリアル : 0001

残りコンテンツ利用回数 : 2

のデータが存在する場合であっても、

【0313】アプリケーション I D : 0001

A C シリアル : 0002

残りコンテンツ利用回数 : 5

の新たな管理データが追加登録される。

【0314】図 39 に、コンテンツ利用可能回数をユーザデバイス内のセキュリティチップで管理する態様とした場合のセキュリティチップ内で実行される利用回数管理データのインポート処理フローを示す。各ステップについて説明する。

【0315】まず、ステップ S 221において、属性証明書（検証済み）からアプリケーション I D、利用制限

回数、属性証明書シリアル番号を取り出す。ステップ S 222において、セキュリティチップ内のメモリに設定済みのサービスプロバイダ管理領域内に、属性証明書に格納されたと同一のアプリケーション I D の回数管理データがあるか否かを検索する。

【0316】ステップ S 223 で、同一のアプリケーション I D の回数管理データの登録がないと判定された場合は、ステップ S 225 に進み、属性証明書に従ってアプリケーション I D : nnnn、属性証明書（A C）シリアル : mmmm、利用可能回数として、受領した属性証明書に記録されたコンテンツ利用制限回数 : x を設定して利用回数管理データ登録を行なう。

【0317】一方、ステップ S 223において、同一のアプリケーション I D の回数管理データが登録済みと判定された場合は、ステップ S 224 に進み、さらに、属性証明書から取得した属性証明書（A C）シリアルと一致する回数管理データがメモリ内のサービスプロバイダ管理領域に登録済みであるか否かを判定し、登録済みである場合は、同一の属性証明書に対する重複処理であると判定して、新たなデータ登録は実行せず処理を終了する。一方、属性証明書から取得した属性証明書（A C）シリアルと一致する回数管理データがメモリ内のサービスプロバイダ管理領域に登録済みでないと判定した場合は、ステップ S 225 に進み、属性証明書に従ってアプリケーション I D : nnnn、属性証明書（A C）シリアル : mmmtt、利用可能回数データとして、受領した属性証明書に記録されたコンテンツ利用制限回数 : x を設定して利用回数管理データの登録を行なう。

【0318】次に、図 40 を参照して、回数管理ファイルをセキュリティチップ外の外部メモリ（例えばハードディスク）に格納管理し、管理データのハッシュ値のみをセキュリティチップ内のメモリに格納する処理態様とした場合の利用回数管理データのインポート処理シーケンスを説明する。左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。図 40 の処理シーケンスは、すでにコンテンツ購入処理に伴うセキュリティチップと、サービスプロバイダ間の相互認証が成立し、サービスプロバイダからセキュリティチップに対する、購入コンテンツに対応する属性証明書の発行処理以降の処理を示している。ここで、サービスプロバイダの発行する属性証明書は、コンテンツ利用条件として、オンライン利用での利用回数制限コンテンツであることが記録され、コンテンツ利用制限回数が記録されている。

【0319】この処理態様は、セキュリティチップ内の限られたメモリ領域を有効に活用する構成であり、回数管理データの実データファイルをセキュリティチップ外の外部メモリ（例えばハードディスク）に格納管理し、この外部管理ファイル情報のハッシュ（Hash）値

を、セキュリティチップ内部で管理することで、外部管理ファイル情報の改竄を検証することを可能としたものである。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、MD4、MD5、SHA-1などが用いられる場合もあるし、DES-CBCが用いられる場合もある。この場合は、最終出力値となるMACがハッシュ値となる。

【0320】図40に示す処理シーケンスについて説明する。（1）属性証明書がサービスプロバイダから発行され、送信されると、（2）セキュリティチップの制御部は、属性証明書の検証処理を実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図20の処理フローと同様のシーケンスに従って実行される。この検証処理において、セキュリティチップの制御部は、属性証明書（AC）内のAC保持者の公開鍵証明書情報を従ってリンクする公開鍵証明書から、上位に辿って連鎖的な検証を行ない、ルート認証局（CA）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【0321】セキュリティチップの制御部は、属性証明書に記録されたコンテンツ利用条件がオフライン利用回数制限コンテンツであると判定すると、外部のメモリからの回数管理ファイルの読み出し処理を実行する。図ではユーザデバイス制御部の管理するHDDに回数管理ファイルがあり、（3）ユーザデバイス制御部において回数管理ファイルが読み出されてセキュリティチップに出力される。この読み出し対象は、管理ファイル全データであっても、あるいはコンテンツに対応するサービスプロバイダに関するデータのみであってもよい。

【0322】次に、セキュリティチップの制御部は、（4）ユーザデバイス制御部から受信した回数管理ファイルをセキュリティチップ内のRAMに展開し、展開データに基づいてハッシュ値を計算する。回数管理データは、サービスプロバイダIDとユーザIDに対応付けられた複数の回数管理データを格納したフィールド構成を持つ。セキュリティチップのメモリ内のサービスプロバイダ管理領域には、サービスプロバイダIDとユーザIDに対応付けられたフィールドデータに対してハッシュ値が生成され格納されている。

【0323】セキュリティチップの制御部は、ユーザデバイス制御部から受信し、RAMに展開した回数管理ファイルから、ユーザにより指定されているサービスプロ

バイダID、ユーザIDに対応するフィールドデータを抽出してハッシュ値を計算し、計算された値と、セキュリティチップ内のメモリのサービスプロバイダ管理領域に格納されたハッシュ値とを比較する。算出ハッシュ値と、格納ハッシュ値が一致すれば、データに改竄がないと判定し、次の処理に進む。

【0324】図の例では、RAM展開データの、サービスプロバイダID：5678、ユーザID：6737のフィールドデータに基づいてハッシュ値が算出され、セキュリティチップ内の対応するサービスプロバイダ（SP）管理領域内に格納された対応するフィールド、すなわち、サービスプロバイダID：5678、ユーザID：6737のハッシュ値：290aと比較することになる。

【0325】（5）ハッシュ値が一致した場合は、一致した旨を示す通知をユーザデバイス制御部に送信し、一致が得られなかった場合はエラーメッセージをユーザデバイス制御部に送信する。（6）次に、セキュリティチップの制御部は、属性証明書からコンテンツ識別子に対応するアプリケーションID、属性証明書（AC）シリアル番号、コンテンツ利用制限回数の各データを取得する。さらに、コンテンツの購入処理時にユーザにより入力されたユーザID、サービスプロバイダIDの各データをユーザデバイス制御部を介して取得し、これらの取得したアプリケーションID、属性証明書（AC）シリアル番号、ユーザIDの各データに対応するコンテンツ利用回数管理データが、ユーザデバイス制御部から受信し、RAMに展開した回数管理ファイルに登録済みであるか否かを検証する。

【0326】コンテンツ利用回数管理データが登録されていないことを確認すると、（7）コンテンツの利用回数管理データを属性証明書（AC）から取り出し、RAMに展開した回数管理ファイルに追加登録し、（8）追加データに基づく新たなハッシュ値を計算して、（9）セキュリティチップ内の対応するサービスプロバイダ（SP）管理領域内に格納された対応するフィールドに格納する。（10）追加登録の終了後、属性証明書受信メッセージを更新した回数管理ファイルとともに、ユーザデバイスに送信し、（11）ユーザデバイスは、受信した回数管理ファイルをハードディスクに格納する。

【0327】図40の例では、サービスプロバイダから受領した属性証明書（AC）は、  
アプリケーションID：0001  
属性証明書（AC）シリアル：1345  
コンテンツ利用制限回数：5  
の各データが記録され、ユーザ入力データは、  
ユーザID：6737  
サービスプロバイダID：5678  
である。

【0328】セキュリティチップの制御部は、これらの

データに対応するコンテンツ利用回数管理データがRAMに展開した回数管理ファイルに登録済みであるか否かを検証する。図40に示す最上段のSC内RAMのデータ中には、サービスプロバイダID：5678、ユーザID：6737に対応するコンテンツ利用回数管理データとして、アプリケーションID：0001、属性証明書(AC)シリアル：1345に対応するデータは存在しない。

【0329】従って、今回サービスプロバイダから受領した属性証明書に対応するコンテンツ利用回数管理データをサービスプロバイダID：5678、ユーザID：6737に対応するコンテンツ利用回数管理データとして、新たに追加する処理を行なう。その結果、図の中段に示すSC内RAMのデータ中に、アプリケーションID：0001、属性証明書(AC)シリアル：1345の回数管理データが追加され、利用可能回数として、受領した属性証明書に記録されたコンテンツ利用制限回数：5が設定される。

【0330】さらに、サービスプロバイダID：5678、ユーザID：6737に対応するフィールドデータに基づいてハッシュ値が算出される。図の例では、データ更新前のハッシュ値は290aであり、データ更新後のハッシュ値が8731であり、図の最下段のSP管理領域のハッシュ値：8731が更新値として格納されることになる。

【0331】コンテンツの利用時には、このコンテンツ利用回数管理データが参照され、利用毎に利用可能回数を1デクリメントして、5→4→3→2→1→0とするデータ更新が実行されるとともに、更新データに基づいて新たなハッシュ値が算出されて、更新処理が実行されることになる。このコンテンツ利用処理については、後述する。

【0332】なお、サービスプロバイダから受領した属性証明書のアプリケーションID、属性証明書(AC)シリアルと同一のデータがすでに、ユーザデバイスから受信し、RAMに展開した回数管理ファイルの対応するサービスプロバイダID、ユーザIDのフィールドのコンテンツ利用回数管理データとして登録済みである場合には、重複した属性証明書の発行であると判定し、その属性証明書に基づくコンテンツ利用回数管理データの追加登録は実行しない。

【0333】また、サービスプロバイダから受領した属性証明書のアプリケーションIDと同一であるが、属性証明書(AC)シリアルが異なるデータがすでに、ユーザデバイスから受信し、RAMに展開した回数管理ファイルの対応するサービスプロバイダID、ユーザIDのフィールドのコンテンツ利用回数管理データとして登録済みである場合には、異なる属性証明書に基づく同一コンテンツの新たな利用を可能とする属性証明書であると判定し、その属性証明書に基づくコンテンツ利用回数管

理データの追加登録、ハッシュ値更新処理を実行する。

【0334】図41に、回数管理ファイルをセキュリティチップ外の外部メモリ(例えばハードディスク)に格納管理し、管理データのハッシュ値のみをセキュリティチップ内のメモリに格納する処理態様とした場合の利用回数管理データのインポート処理フローを示す。各ステップについて説明する。

【0335】まず、ステップS241において、外部メモリから回数管理ファイルを読み込み、ステップS242において、サービスプロバイダID、ユーザIDに基づいて特定されるフィールドデータに基づくハッシュ値を算出し、算出ハッシュ値と、セキュリティチップのメモリ内のサービスプロバイダ管理領域に格納済みのハッシュ値と一致するか否かを検証(S243)する。一致しない場合は、外部メモリから読み出した回数管理ファイルが改竄されていると判定し、エラー処理、例えばその後の処理を中止する。

【0336】ハッシュ値が一致し、外部メモリから読み出した回数管理ファイルが改竄されていないと判定した場合は、ステップS244に進み、属性証明書(検証済み)からアプリケーションID、利用制限回数、属性証明書シリアル番号を取り出す。次に、ステップS245において、ユーザデバイス制御部から受信し、RAMに展開した回数管理ファイルに、属性証明書に格納されたものと同一のアプリケーションIDの回数管理データがあるか否かを検索する。

【0337】ステップS246で、同一のアプリケーションIDの回数管理データの登録がないと判定された場合は、ステップS247に進み、属性証明書に従ってアプリケーションID：nnnn、属性証明書(AC)シリアル：mmmm、利用可能回数として、受領した属性証明書に記録されたコンテンツ利用制限回数：xを設定して利用回数管理データの登録を行なう。

【0338】一方、ステップS246において、同一のアプリケーションIDの回数管理データの登録が登録済みと判定された場合は、ステップS251に進み、さらに、属性証明書から取得した属性証明書(AC)シリアルと一致する回数管理データがRAMに展開した回数管理ファイルに登録済みであるか否かを判定し、登録済みである場合は、同一の属性証明書に対する重複処理であると判定して、新たなデータ登録は実行せず処理を終了する。一方、属性証明書から取得した属性証明書(AC)シリアルと一致する回数管理データがRAMに展開した回数管理ファイルに登録済みでないと判定した場合は、ステップS247に進み、属性証明書に従ってアプリケーションID：nnnn、属性証明書(AC)シリアル：mmmm、利用可能回数として、受領した属性証明書に記録されたコンテンツ利用制限回数：xを設定して利用回数管理データ登録を行なう。

【0339】ステップS247において、属性証明書に

従って、新たな回数管理データが、RAMに展開した回数管理ファイルに書き込まれると、ステップS248において、新規追加データを含めたデータに基づいて新たなハッシュ値が計算され、新たなハッシュ値をセキュリティチップ内の対応するサービスプロバイダ(SP)管理領域内に格納された対応するフィールドに格納する。さらに、ステップS249において、更新した回数管理ファイルに基づいて外部メモリ(例えばハードディスク)に格納された回数管理ファイルの更新が実行される。

【0340】次に、属性証明書に記録されたコンテンツ利用条件がオンライン処理であり、利用回数制限コンテンツである場合の属性証明書の取得から、コンテンツ取得までの処理を図42のシーケンス図に従って説明する。

【0341】図42に示す処理シーケンスは、先に説明した図34、図35、図36の処理シーケンスと同様、すでにサービスプロバイダから暗号化コンテンツを受領済みであり、また、コンテンツに対応する利用条件、暗号化コンテンツ鍵を格納した属性証明書を受領済みであるユーザデバイスにおける処理を示しており、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部(上位ソフトウェア)、およびサービスプロバイダの処理を示している。

【0342】図42に示す処理中、最上段(a)は、属性証明書がセキュリティチップの内部メモリに格納されている場合における属性証明書からのサービスプロバイダID取得処理、(b)は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダID取得処理を示し、これら(a)、(b)は属性証明書の格納位置に応じて選択的に行われる。(a)、(b)の各処理は、図34を参照して説明したオンライン期間制限の場合の処理と同様であるので説明を省略する。(a)、(b)のいずれかの処理によって、サービスプロバイダIDが取得されると、次に、図42(c)に示す処理、すなわちコンテンツ取得処理を実行する。

【0343】(c1)ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報(コンテンツ利用条件)を確認し、属性証明書を適用したコンテンツ利用要求をセキュリティチップに対して出力する。この例における属性証明書に記録されたコンテンツ利用条件は、オンライン利用回数制限である。

【0344】(c2)セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書(AC)適用要求を受信すると、属性証明書の検証処理を実行する。検証処理には、権限情報(コンテンツ利用条件)の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図20の処理フローと同様の

シーケンスに従って実行される。この検証処理において、セキュリティチップの制御部は、属性証明書(AC)内のAC保持者の公開鍵証明書情報を従ってリンクする公開鍵証明書から、上位に辿って連鎖的な検証を行ない、ルート認証局(CA)の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【0345】(c3)属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップ制御部は、回数管理データの更新処理を実行する。回数管理データの更新処理の詳細については、後述する。さらに、セキュリティチップ制御部は、(c4)属性証明書内に格納された暗号化コンテンツ鍵:[SC. St o p u b. SP. K(Kc)]を取り出して、サービスプロバイダ管理領域に格納されたSP対応ストレージ秘密鍵:SC. St o p r i. SP. Kを適用して復号化処理を実行し、コンテンツ鍵:Kcを取得する。コンテンツ鍵:Kcの取得に成功すると、セキュリティチップ制御部は、ユーザデバイス制御部にコンテンツの復号準備が完了したことを通知する。

【0346】(c5)次にユーザデバイス制御部は、取得したコンテンツ鍵を適用して復号すべき暗号化コンテンツ[Kc(Content)]をユーザデバイス内のメモリ(例えばハードディスク)、あるいはセキュリティチップ制御部を介してセキュリティチップ内のメモリから取得する。さらに、取得した暗号化コンテンツをセキュリティチップに送信し、(c6)セキュリティチップ内で暗号化コンテンツに対してコンテンツ鍵:Kcを適用した復号化処理を実行し、復号化処理結果として得られるコンテンツをユーザデバイス制御部に出力し、(c7)ユーザデバイスは、コンテンツを取得する。これらの処理が終了すると、(c8)セキュリティチップの制御部は、復号化処理によって取得したコンテンツ鍵:Kc、およびコンテンツ(Content)を破棄する。

【0347】これらの処理によって、属性証明書(AC)に基づくコンテンツの利用回数制限内のコンテンツ利用である場合に限り、コンテンツ鍵:Kcがセキュリティチップにおいて復号され、コンテンツ鍵が取得され、取得したコンテンツ鍵によるコンテンツの復号が実行されてユーザデバイスにおいてコンテンツ利用が可能となる。

【0348】なお、上記構成例では、公開鍵暗号方式を適用し、コンテンツ鍵の暗号化にSP対応ストレージ公開鍵:SC. St o p u b. SP. Kを用い、コンテンツ鍵の復号にSP対応ストレージ秘密鍵:SC. St o p r i. SP. Kを用いた構成としたが、共通鍵方式を適用することも可能であり、共通鍵方式を適用する場合は、コンテンツ鍵の暗号化、復号化の双方の処理にSP対応ストレージ鍵(共通鍵):SC. St o. SP. K

を用いる。この場合、S P 対応ストレージ鍵（共通鍵）：S C. S t o. S P. K は、セキュリティチップのメモリの対応するサービスプロバイダのサービスプロバイダ管理領域に格納される。

【0349】なお、サービスプロバイダからユーザデバイスに対するコンテンツ配信あるいは属性証明書（A C : Attribute Certificate）の配信形態としては、ユーザ側からサービスプロバイダに対する要求に基づいて実行される形態と、ユーザの要求の有無に関係なく例えばサブスクライバ契約を結んでいるユーザに対して、サービスプロバイダから一方的に送信するいわゆるプッシュ型の形態（プッシュ型モデル）のいずれの形態も可能である。プッシュ型モデルにおいては、サービスプロバイダが予め目標ユーザ向けの属性証明書（A C）を作成して配信することになる。

【0350】次に、図43、図44を参照して、利用回数管理データの更新処理について説明する。コンテンツ利用可能回数の管理態様には、前述したようにコンテンツ利用可能回数をユーザデバイス内のセキュリティチップで管理する態様と、回数管理ファイルをセキュリティチップ外の外部メモリ（例えばハードディスク）に格納管理し、管理データのハッシュ値のみをセキュリティチップ内のメモリに格納する2つの態様がある。図43は前者、図44は後者の態様における回数管理データの更新処理シーケンスを説明する図である。

【0351】最初に図43を参照して、コンテンツ利用可能回数をユーザデバイス内のセキュリティチップで管理する態様とした場合の回数管理データの更新処理シーケンスを説明する。左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）の処理を示している。図43の処理シーケンスは、すでにセキュリティチップ内で属性証明書の検証が済んでいるものとして、その後の処理を示している。

【0352】（1）セキュリティチップの制御部は、検証済みの属性証明書に記録されたコンテンツ利用条件がオンライン利用回数制限コンテンツであると判定すると、属性証明書からコンテンツ識別子に対応するアプリケーションID、属性証明書（A C）シリアル番号、コンテンツ利用制限回数の各データを取得する。さらに、コンテンツの購入処理時にユーザにより入力されたユーザID、サービスプロバイダIDの各データをユーザデバイス制御部を介して取得し、これらの取得したアプリケーションID、属性証明書（A C）シリアル番号、ユーザIDの各データに対応するコンテンツ利用回数管理データが、セキュリティチップ内のメモリのサービスプロバイダ管理領域に登録済みであるか否かを検証する。

【0353】セキュリティチップのメモリには、前述したように、登録されたサービスプロバイダ毎にサービスプロバイダ管理領域が設定され、その管理領域内にコンテンツ利用回数管理データが登録されることになる。

【0354】図43に示す例では、属性証明書（A C）は、

アプリケーションID : 0002

属性証明書（A C）シリアル : 3278

コンテンツ利用制限回数 : 10

の各データが記録され、ユーザ入力データは、

ユーザID : 6737

サービスプロバイダID : 5678

である。

10 【0355】セキュリティチップの制御部は、これらのデータに対応するコンテンツ利用回数管理データがメモリ内の対応するサービスプロバイダ管理領域にあるか否かを検証する。図43に示すS P管理領域データ（更新前）のデータ中には、サービスプロバイダID : 5678、ユーザID : 6737に対応するコンテンツ利用回数管理データとして、アプリケーションID : 0002、属性証明書（A C）シリアル : 3278に対応するデータが存在し、利用可能回数（残回数） : 7と設定されている。

20 【0356】（2）セキュリティチップ制御部は、この抽出データから利用可能回数（残回数） : 7 > 0であること、さらに、属性証明書に記録された制限回数以下、 $10 \geq 7$ であることを確認し、これらが確認されたことを条件としてコンテンツの利用を許可、すなわち、属性証明書に格納された（3）暗号化コンテンツ鍵の復号化処理を実行する。

【0357】（4）さらに、セキュリティチップ制御部は、メモリ内の対応するサービスプロバイダ管理領域の対応データの利用可能回数を1減少させるデータ更新処理を実行する。この場合は、アプリケーションID : 0002、属性証明書（A C）シリアル : 3278に対応するデータ中の、利用可能回数（残回数） : 7を6に更新する処理を実行する。なお、（3）の暗号化コンテンツ鍵の復号化処理と、（4）の回数管理データの更新処理は、処理手順を（4）を先に（3）を後にする構成としてもよく、また並列に実行してもよい。

【0358】次に、図44を参照して、回数管理ファイルをセキュリティチップ外の外部メモリ（例えばハードディスク）に格納管理し、管理データのハッシュ値のみをセキュリティチップ内のメモリに格納する態様とした場合の回数管理データの更新処理シーケンスを説明する。左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）の処理を示している。図44の処理シーケンスは、すでにセキュリティチップ内で属性証明書の検証が済んでいるものとして、その後の処理を示している。

【0359】セキュリティチップの制御部は、属性証明書に記録されたコンテンツ利用条件がオンライン利用回数制限コンテンツであると判定すると、外部のメモリからの回数管理ファイルの読み出し処理を実行する。図で

はユーザデバイス制御部の管理するHDDに回数管理ファイルがあり、(1)ユーザデバイス制御部において回数管理ファイルが読み出されてセキュリティチップに出力される。この読み出し対象は、管理ファイル全データであっても、あるいはコンテンツに対応するサービスプロバイダに関するデータのみであってもよい。

【0360】次に、セキュリティチップの制御部は、(2)ユーザデバイス制御部から受信した回数管理ファイルをセキュリティチップ内のRAMに展開し、展開データに基づいてハッシュ値を計算する。回数管理データは、サービスプロバイダIDとユーザIDに対応付けられた複数の回数管理データを格納したフィールド構成を持つ。セキュリティチップのメモリ内のサービスプロバイダ管理領域には、サービスプロバイダIDとユーザIDに対応付けられたフィールドデータに対してハッシュ値が生成され格納されている。

【0361】セキュリティチップの制御部は、ユーザデバイスから受信し、RAMに展開した回数管理ファイルから、ユーザにより指定されているサービスプロバイダID、ユーザIDに対応するフィールドデータを抽出してハッシュ値を計算し、計算された値と、セキュリティチップ内のメモリのサービスプロバイダ管理領域に格納されたハッシュ値とを比較する。算出ハッシュ値と、格納ハッシュ値が一致すれば、データに改竄がないと判定し、次の処理に進む。

【0362】図の例では、RAM展開データの、サービスプロバイダID：5678、ユーザID：6737のフィールドデータに基づいてハッシュ値が算出され、セキュリティチップ内の対応するサービスプロバイダ(SP)管理領域内に格納された対応するフィールド、すなわち、サービスプロバイダID：5678、ユーザID：6737のハッシュ値：8731と比較することになる。

【0363】(3)ハッシュ値が一致した場合は、一致した旨を示す通知をユーザデバイスに送信し、一致が得られなかった場合はエラーメッセージをユーザデバイスに送信する。(4)次に、セキュリティチップの制御部は、属性証明書からコンテンツ識別子に対応するアプリケーションID、属性証明書(AC)シリアル番号、コンテンツ利用制限回数の各データを取得する。さらに、コンテンツの購入処理時にユーザにより入力されたユーザID、サービスプロバイダIDの各データをユーザデバイス制御部を介して取得し、これらの取得したアプリケーションID、属性証明書(AC)シリアル番号、ユーザIDの各データに対応するコンテンツ利用回数管理データが、ユーザデバイスから受信し、RAMに展開した回数管理ファイルに登録済みであるか否かを検証する。

【0364】図44に示す例では、属性証明書(AC)は、

アプリケーションID：0002

属性証明書(AC)シリアル：3278

コンテンツ利用制限回数：10

の各データが記録され、ユーザ入力データは、ユーザID：6737

サービスプロバイダID：5678

である。

【0365】セキュリティチップの制御部は、これらのデータに対応するコンテンツ利用回数管理データがRAMに展開した回数管理ファイルに登録済みであるか否かを検証する。図44に示す最上段のSC内RAMのデータ中には、サービスプロバイダID：5678、ユーザID：6737に対応するコンテンツ利用回数管理データとして、アプリケーションID：0002、属性証明書(AC)シリアル：3278に対応するデータが存在し、利用可能回数(残回数)：7と設定されている。

【0366】(5)セキュリティチップ制御部は、この抽出データから利用可能回数(残回数)：7>0であること、さらに、属性証明書に記録された制限回数以下、10≥7であることを確認し、これらが確認されたことを条件としてコンテンツの利用を許可、すなわち、属性証明書に格納された(6)暗号化コンテンツ鍵の復号化処理を実行する。

【0367】(7)さらに、セキュリティチップ制御部は、RAMに展開した回数管理ファイルの対応データの利用可能回数を1減少させるデータ更新処理を実行する。この場合は、アプリケーションID：0002、属性証明書(AC)シリアル：3278に対応するデータ中の、利用可能回数(残回数)：7を6に更新する処理を実行する。

【0368】さらに、セキュリティチップ制御部は、(8)更新データに基づく新たなハッシュ値を計算して、(9)セキュリティチップ内の対応するサービスプロバイダ(SP)管理領域内に格納された対応するフィールドに格納する。図44の例では、更新前のアプリケーションID：0002、属性証明書(AC)シリアル：3278に対応するフィールドデータに基づくハッシュ値は8731であり、更新後の同フィールドのデータに基づくハッシュ値はbc35となり、サービスプロバイダID：5678、ユーザID：6737に対応する図の最下段のSP管理領域のハッシュ値：bc35が更新ハッシュ値として格納されることになる。

【0369】(10)更新処理の終了後、更新した回数管理ファイルを、ユーザデバイス制御部に送信し、ユーザデバイス制御部は、受信した回数管理ファイルをハードディスクに格納する。

【0370】このように、コンテンツの利用時には、このコンテンツ利用回数管理データが参照され、利用毎に利用可能回数を1デクリメントして、5→4→3→2→1→0とするデータ更新が実行されるとともに、更新デ

ータに基づいて新たなハッシュ値が算出されて、更新処理が実行され、属性証明書に記録された利用制限回数内のコンテンツ利用が可能となる。

【0371】以上、属性証明書のコンテンツ利用条件に従ったコンテンツの利用について説明した。なお、上記説明においては、期間制限と回数制限とを別々に説明したが、期間制限と回数制限の両制限を持つ属性証明書も可能であり、これらの場合は2つの条件に基づいてコンテンツ利用可否を判定した上で、属性証明書に設定された利用条件内の期限内、回数内のコンテンツ利用であることの確認を条件として、コンテンツ鍵の復号を行なうものとする。

【0372】[アップグレード処理] 属性証明書には、コンテンツの利用条件として期間制限、回数制限、買い切り等の各種利用条件が設定され、これらの利用条件に基づいてセキュリティチップを持つユーザデバイスにおいてコンテンツの利用が行なわれることを説明した。次に、例えば属性証明書に設定されたコンテンツ利用制限回数の変更、あるいは期間制限の延長など、コンテンツの利用制限を変更する処理、すなわちアップグレード処理について説明する。

【0373】アップグレード処理には、具体的には、以下に説明する各種の態様がある。

(1) 利用回数制限をコンテンツ利用条件として記録した属性証明書の利用可能回数を増やす。例えば、10回券を買って、5回残っていて、10回に増やす。10回券を買って、使い切って、10回券に増やす。

(2) 利用期間制限をコンテンツ利用条件として記録した属性証明書の利用期間を延長する。例えば、1週間後までしか使えないものを、1ヶ月後まで使えるように期間を延長する。期間が切れて使えなくなったものを、1ヶ月後まで使えるように期間を延長する。

(3) 回数制限や期間制限をコンテンツ利用条件として記録した属性証明書の利用条件の変更。例えば、回数制限を期間制限に変更する。期間制限を回数制限に変更する。回数制限を買い切りに変更する。期間制限を買い切りに変更する。

(4) アルバム化アップグレード一連のアルバム化されたコンテンツデータ、例えば1枚のCDあるいはDVD等に格納された複数(n)のコンテンツ1~n、あるいは何らかのシリーズ化されたコンテンツ1~nがあり、これらのいくつかを購入済であり、購入済みコンテンツに対応する属性証明書1~属性証明書nの複数をユーザがユーザデバイス内に保持している場合、例えば、コンテンツ1に対応する属性証明書1、コンテンツ3に対応する属性証明書3、コンテンツ5に対応する属性証明書5、をユーザデバイスに保持している場合、これらの属性証明書をサービスプロバイダに提示することにより、アルバムを構成する他のコンテンツ、すなわち、コンテンツ2、4、6~nのコンテンツを割引価格で一括(ア

ルバム) 購入できる。

【0374】属性証明書に基づくアップグレード処理には、上述した様々な態様がある。このアップグレード処理の実行シーケンスの概略は、次の通りである。まず、サービスプロバイダ(SP)がアップグレードメニューをユーザデバイスに提示し、ユーザがアップグレードメニューを選択する。ユーザデバイスは、ユーザの指定に従って、アップグレード処理対象とする取得済みの属性証明書の指定データとともに、アップグレード要求コマンドをセキュリティチップに送信する。セキュリティチップの制御部は、サービスプロバイダとの通信を実行して、アップグレード処理対象とする取得済みの属性証明書をサービスプロバイダに送信する。サービスプロバイダは、受信した属性証明書を検証した後、ユーザの指定したアップグレード処理を実行し、新たな属性証明書を発行しセキュリティチップに送信する。ユーザデバイスでは、新たな属性証明書の利用条件に従ってコンテンツを利用することが可能となる。

【0375】以下、アップグレードのベースとして用いる属性証明書(AC)に記載されたコンテンツ利用条件が以下の3態様である場合のアップグレード処理について、順次、説明する。

- (A) オンライン-利用期間制限コンテンツ
- (B) オンライン-利用回数制限コンテンツ
- (C) オフライン-利用回数制限コンテンツ

【0376】(A) オンライン-利用期間制限属性証明書(AC)をベースとしたアップグレード処理  
まず、属性証明書に記録されたコンテンツ利用条件がオンライン処理であり、利用期間制限が設定された属性証明書を保有する場合、このオンライン-利用期間制限属性証明書をベースとしたアップグレード処理を図45のシーケンス図に従って説明する。図45には、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部(上位ソフトウェア)、およびサービスプロバイダの処理を示している。

【0377】図45では、最上段(a)は、属性証明書がセキュリティチップの内部メモリに格納されている場合における属性証明書からのサービスプロバイダID取得処理、(b)は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダID取得処理を示し、これら(a)、(b)は属性証明書の格納位置に応じて選択的に行なわれる。(c)の相互認証処理、(d)のコンテンツ取得処理は共通に行なわれる。

【0378】まず、(a)の処理から説明する。(a)  
1) ユーザデバイス制御部は、アップグレード処理対象の属性証明書の検索をセキュリティチップ制御部に要求する。(a2) セキュリティチップ制御部は、チップのメモリに格納済みの属性証明書のリストをユーザデバイ

ス制御部に出力し、(a 3) ユーザデバイスでは付属のブラウザによりリストを表示する。(a 4) ユーザは表示されたリストからアップグレード処理対象の属性証明書(AC)を指定し、読み出し命令をセキュリティチップ制御部に送信する。(a 5) セキュリティチップ制御部は、指定された属性証明書を内部メモリから読み出してユーザデバイス制御部に出力し、(a 6) ユーザデバイスでは付属のブラウザにより属性証明書を表示し、属性証明書格納データ中のサービスプロバイダ識別子(SPID)を取得する。

【0379】属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合は、(b)の処理となる。(b 1) ユーザデバイス制御部は、アップグレード処理対象の属性証明書の検索を実行し、(b 2) ユーザデバイスでは付属のブラウザにより表示されたACリストからアップグレード処理対象の属性証明書(AC)を指定し、読み出して属性証明書を表示し、(b 4) 属性証明書格納データ中のサービスプロバイダ識別子(SPID)を取得する。

【0380】上記(a)、(b)のいずれかの処理によって取得されたサービスプロバイダ識別子(SPID)は、サービスプロバイダ管理領域から、相互認証に必要な情報を取得するために用いられる。前述したように、サービスプロバイダ管理領域へのアクセスにはサービスプロバイダ毎に設定されたパスワード入力が必要であり、ユーザは、属性証明書から取得したサービスプロバイダ識別子(SPID)に対応するパスワード入力により、サービスプロバイダ管理領域へのアクセスを実行し、図45の(c 1)に示すセキュリティチップとサービスプロバイダ間の相互認証処理を実行する。

【0381】この相互認証処理は、先に説明した図16のTLS1.0処理または、その他の方式、例えば公開鍵方式による相互認証処理として実行される。この相互認証処理においては、相互の公開鍵証明書の検証がなされ、必要に応じてルート認証局(CA)までの公開鍵証明書が連鎖的に検証される。この認証処理において、セキュリティチップと、サービスプロバイダはセッション鍵(Kses)を共有する。相互認証が成立すると、次に、図45(d)に示す処理、すなわちアップグレード属性証明書取得処理を実行する。

【0382】(d 1) ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報(コンテンツ利用条件)を確認し、属性証明書のアップグレード適用要求と、アップグレード条件をセキュリティチップに対して出力する。この例におけるアップグレード処理対象の属性証明書に記録されたコンテンツ利用条件は、オンライン期間制限であり、ユーザの指定するアップグレード条件は、例えば、

期間制限の変更(延長)

期間制限→オンライン回数制限へ変更  
期間制限→オフライン回数制限へ変更  
期間制限→買い切りへ変更  
等の条件である。

【0383】(d 2) セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書(AC)アップグレード適用要求を受信すると、属性証明書の検証処理を実行する。検証処理には、権限情報(コンテンツ利用条件)の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図20の処理フローと同様のシーケンスに従って実行される。

【0384】さらに、必要に応じてセキュリティチップの制御部は、属性証明書(AC)内のAC保持者の公開鍵証明書情報に従ってリンクする公開鍵証明書を取得して、公開鍵証明書の検証を行なうことが好ましい。例えば属性証明書(AC)の発行者の信頼度が不確かである場合には、属性証明書(AC)の発行者の公開鍵証明書の検証を行なうことによって、認証局の公開鍵証明書を正当に有しているか否かの判定が可能となる。なお、公開鍵証明書が前述したように階層構成をなしている場合は、経路を上位に辿って連鎖的な検証を行ない、ルート認証局(CA)の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【0385】(d 3) 属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード処理対象の属性証明書を、ユーザにより指定されたアップグレード条件情報とともに送付する。アップグレード処理対象の属性証明書には、利用条件としてオンライン期間制限コンテンツであることが記録され、また有効期限データが格納されている。さらに、サービスプロバイダの保有する秘密鍵:SP.S to.Kで暗号化されたコンテンツ鍵のデータ、すなわち、[SP.S to.K(Kc)]が格納されている。

【0386】(d 4) セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、(d 5) ユーザにより指定されたアップグレード条件情報に基づくアップグレード属性証明書生成処理を実行する。

【0387】アップグレード属性証明書生成処理は、ユーザにより指定されたコンテンツ利用条件を記録した新たな属性証明書、すなわちセキュリティチップから受信した属性証明書と異なるシリアル番号を持つ属性証明書を発行する処理として実行する。なお、この際、新たに発行するアップグレード属性証明書中には、アップグレード属性証明書生成処理によって生成された属性証明書の属性情報を記録する。

ードのベースとなった属性証明書のシリアルを含む履歴データを格納する。

【0388】なお、アップグレードの態様は、前述したように、

期間制限の変更（延長）

期間制限→オンライン回数制限へ変更

期間制限→オフライン回数制限へ変更

期間制限→買い切りへ変更

のいずれかであり、期間制限の変更の場合は、利用期間を新たに設定したアップグレード属性証明書を生成する。また、オンラインまたはオフライン回数制限へ変更する場合は、利用制限回数を格納したアップグレード属性証明書を生成する。また、買い切りへ変更する場合は、コンテンツ利用条件を買い切りとしたアップグレード属性証明書を生成する。

【0389】期間制限の変更、あるいはオンライン回数制限へ変更する場合は、アップグレード属性証明書に格納するコンテンツ鍵は、元の属性証明書と同様、サービスプロバイダの秘密鍵で暗号化したコンテンツ鍵〔S P. S t o. K (K c)〕として格納するが、オフライン回数制限へ変更、または買い切りへ変更する場合は、アップグレード属性証明書には、元の属性証明書とは異なり、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたS P対応ストレージ秘密鍵：S C. S t o p r i. S P. Kに対応する公開鍵で暗号化したコンテンツ鍵、すなわち、〔S C. S t o p u b. S P. K (K c)〕を格納する。

【0390】なお、オフライン処理とする場合であって、公開鍵方式ではなく、共通鍵方式の適用を行なっている場合は、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたS P対応ストレージ鍵（共通鍵）によって暗号化したコンテンツ鍵を格納する。なお、サービスプロバイダがこの共通鍵を保有していない場合は、図45のステップ（d3）のセキュリティチップからサービスプロバイダへの属性証明書の送付時に、併せてS P対応ストレージ鍵（共通鍵）を送付する。この場合は、相互認証時に生成したセッション鍵で暗号化して送付する。

【0391】サービスプロバイダは、アップグレード属性証明書を生成すると、これをセキュリティチップに送付する。

【0392】（d6）セキュリティチップ制御部は、サービスプロバイダからのアップグレード属性証明書（A C）を受信すると、属性証明書の検証処理を実行する。検証処理には、格納された権限情報（コンテンツ利用条件）が指定条件と一致するかの確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図20の処理フローと同様のシーケンスに従って実行される。さらに、必要に応じてセキュリティチップの制御部は、属性証明書（A C）内のA C保持者

の公開鍵証明書情報を従って、公開鍵証明書の連鎖検証を行なうことが好ましい。なお、この連鎖検証が必須の場合もある。

【0393】（d7）属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード属性証明書受信確認を送信し、（d8）アップグレード属性証明書をメモリに格納する。

【0394】さらに、セキュリティチップの制御部は、10アップグレード属性証明書がオフライン回数制限である場合には、コンテンツの利用時までに前述した利用回数管理データのインポート処理を実行する。利用回数管理データのインポート処理の詳細は、先に図37～図41を参照して説明した通りであり、セキュリティチップ内部に利用可能回数を格納する態様と、外部メモリに利用可能回数を格納し、セキュリティチップにハッシュ値のみを格納する態様がある。

【0395】以上の処理により、ユーザデバイスは、すでに保持する属性証明書に基づいて新たなアップグレード属性証明書を取得し、アップグレード属性証明書に従った利用条件にしたがったコンテンツの利用が可能となる。

【0396】（B）オンライン-利用回数制限属性証明書（A C）をベースとしたアップグレード処理  
次に、属性証明書に記録されたコンテンツ利用条件がオンライン処理であり、利用回数制限が設定された属性証明書を保有する場合、このオンライン-利用回数制限属性証明書をベースとしたアップグレード処理を図46のシーケンス図に従って説明する。図46には、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）、およびサービスプロバイダの処理を示している。

【0397】図46では、最上段（a）は、属性証明書がセキュリティチップの内部メモリに格納されている場合における属性証明書からのサービスプロバイダID取得処理。（b）は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダID取得処理を示し、（c）はセキュリティチップとサービスプロバイダの相互認証処理である。これらの処理は、前述の図45の場合と同様であり、説明を省略する。

【0398】相互認証後成立後の処理から説明する。  
（d1）ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報（コンテンツ利用条件）を確認し、属性証明書のアップグレード適用要求と、アップグレード条件をセキュリティチップに対して出力する。この例におけるアップグレード処理対象の属性証明書に記録されたコンテンツ利用条件は、オンライン回数制限であり、ユーザの指定するアップグレード条

件は、例えば、

利用可能回数の変更（回数増加）

オンライン回数制限→期間制限へ変更

オンライン回数制限→オフライン回数制限へ変更

オンライン回数制限→買い切りへ変更

等の条件である。

【0399】(d2) セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書(AC)アップグレード適用要求を受信すると、属性証明書の検証処理を実行する。検証処理には、権限情報(コンテンツ利用条件)の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図20の処理フローと同様のシーケンスに従って実行される。さらに、必要に応じてセキュリティチップの制御部は、属性証明書(AC)内のAC保持者の公開鍵証明書、さらに、連鎖公開鍵証明書の検証を行ない、ルート認証局(CA)の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【0400】(d3) 属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード処理対象の属性証明書を、ユーザにより指定されたアップグレード条件情報とともに送付する。アップグレード処理対象の属性証明書には、利用条件としてオンライン回数制限コンテンツであることが記録され、また利用制限回数が格納されている。さらに、サービスプロバイダの保有する秘密鍵: S.P. S.t.o. Kで暗号化されたコンテンツ鍵のデータ、すなわち、[S.P. S.t.o. K (Kc)]が格納されている。

【0401】(d4) セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、(d5)ユーザにより指定されたアップグレード条件情報に基づくアップグレード属性証明書生成処理を実行する。

【0402】アップグレード属性証明書生成処理は、ユーザにより指定されたコンテンツ利用条件を記録した新たな属性証明書、すなわちセキュリティチップから受信した属性証明書と異なるシリアル番号を持つ属性証明書を発行する処理として実行する。なお、この際、新たに発行するアップグレード属性証明書中には、アップグレードのベースとなった属性証明書のシリアルを含む履歴データを格納する。

【0403】なお、アップグレードの態様は、前述したように、

利用制限回数の変更（回数増加）

オンライン回数制限→期間制限へ変更

オンライン回数制限→オフライン回数制限へ変更

オンライン回数制限→買い切りへ変更

のいずれかであり、回数制限の変更の場合は、利用制限回数を新たに設定したアップグレード属性証明書を生成する。また、期間制限へ変更する場合は、期間制限情報を格納したアップグレード属性証明書を生成する。

【0404】オンライン回数制限として利用制限回数を変更する場合、期間制限へ変更する場合は、アップグレード属性証明書に格納するコンテンツ鍵は、元の属性証明書と同様、サービスプロバイダの秘密鍵で暗号化したコンテンツ鍵[S.P. S.t.o. K (Kc)]として格納するが、オフライン回数制限へ変更、または買い切りへ変更する場合は、アップグレード属性証明書には、元の属性証明書とは異なり、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたSP対応ストレージ秘密鍵: S.C. S.t.o.p.r.i. S.P. Kに対応する公開鍵で暗号化したコンテンツ鍵、すなわち、[S.C. S.t.o.p.u.b. S.P. K (Kc)]を格納する。

【0405】なお、オフライン処理とする場合であって、公開鍵方式ではなく、共通鍵方式の適用を行なっている場合は、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたSP対応ストレージ鍵(共通鍵)によって暗号化したコンテンツ鍵を格納する。なお、サービスプロバイダがこの共通鍵を保有していない場合は、図46のステップ(d3)のセキュリティチップからサービスプロバイダへの属性証明書の送付時に、併せてSP対応ストレージ鍵(共通鍵)を送付する。この場合は、相互認証時に生成したセッション鍵で暗号化して送付する。

【0406】サービスプロバイダは、アップグレード属性証明書を生成すると、これをセキュリティチップに送付する。

【0407】(d6) セキュリティチップ制御部は、サービスプロバイダからのアップグレード属性証明書(AC)を受信すると、属性証明書の検証処理を実行する。検証処理には、格納された権限情報(コンテンツ利用条件)が指定条件と一致するかの確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図20の処理フローと同様のシーケンスに従って実行される。さらに、必要に応じてセキュリティチップの制御部は、属性証明書(AC)内のAC保持者の公開鍵証明書情報を従って、公開鍵証明書の連鎖検証を行なうことが好ましい。なお、この連鎖検証が必須の場合もある。

【0408】(d7) 属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード属性証明書受信確認を送信し、(d8)アップグレ

ード属性証明書をメモリに格納する。

【0409】さらに、セキュリティチップの制御部は、アップグレード属性証明書がオンライン回数制限である場合には、コンテンツの利用時までに前述した利用回数管理データのインポート処理を実行する。利用回数管理データインポート処理の詳細は、先に図37～図41を参照して説明した通りであり、セキュリティチップ内部に利用可能回数を格納する様と、外部メモリに利用可能回数を格納し、セキュリティチップにハッシュ値のみを格納する様がある。

【0410】以上の処理により、ユーザデバイスは、すでに保持する属性証明書に基づいて新たなアップグレード属性証明書を取得し、アップグレード属性証明書に従った利用条件にしたがったコンテンツの利用が可能となる。

【0411】(C) オフライン-利用回数制限属性証明書(AC)をベースとしたアップグレード処理  
次に、属性証明書に記録されたコンテンツ利用条件がオフライン処理であり、利用回数制限が設定された属性証明書を保有する場合、このオフライン-利用回数制限属性証明書をベースとしたアップグレード処理を図47のシーケンス図に従って説明する。図47には、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部(上位ソフトウェア)、およびサービスプロバイダの処理を示している。

【0412】図47では、最上段(a)は、属性証明書がセキュリティチップの内部メモリに格納されている場合における属性証明書からのサービスプロバイダID取得処理、(b)は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダID取得処理を示し、(c)はセキュリティチップとサービスプロバイダの相互認証処理である。これらの処理は、前述の図45の場合と同様であり、説明を省略する。

【0413】相互認証後成立後の処理から説明する。

(d1) ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報(コンテンツ利用条件)を確認し、属性証明書のアップグレード適用要求と、アップグレード条件をセキュリティチップに対して出力する。この例におけるアップグレード処理対象の属性証明書に記録されたコンテンツ利用条件は、オンライン回数制限であり、ユーザの指定するアップグレード条件は、例えば、

利用可能回数の変更(回数増加)

オンライン回数制限→期間制限へ変更

オンライン回数制限→オンライン回数制限へ変更

オンライン回数制限→買い切りへ変更等の条件である。

【0414】(d2) セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書(AC)アップグ

レード適用要求を受信すると、属性証明書の検証処理を実行する。検証処理には、権限情報(コンテンツ利用条件)の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図20の処理フローと同様のシーケンスに従って実行される。さらに、必要に応じてセキュリティチップの制御部は、属性証明書(AC)内のAC保持者の公開鍵証明書、さらに、連鎖公開鍵証明書の検証を行ない、ルート認証局(CA)の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【0415】(d3) 属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード処理対象の属性証明書を、ユーザにより指定されたアップグレード条件情報とともに送付する。アップグレード処理対象の属性証明書には、利用条件としてオンライン回数制限コンテンツであることが記録され、また利用制限回数が格納されている。さらに、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたSP対応ストレージ秘密鍵:SC.S top r i.S P.Kに対応する公開鍵で暗号化したコンテンツ鍵、すなわち、[SC.S top u b.S P.K(Kc)]が格納されている。

【0416】(d4) セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、(d5)ユーザにより指定されたアップグレード条件情報に基づくアップグレード属性証明書生成処理を実行する。

【0417】アップグレード属性証明書生成処理は、ユーザにより指定されたコンテンツ利用条件を記録した新たな属性証明書、すなわちセキュリティチップから受信した属性証明書と異なるシリアル番号を持つ属性証明書を発行する処理として実行する。なお、この際、新たに発行するアップグレード属性証明書中には、アップグレードのベースとなった属性証明書のシリアルを含む履歴データを格納する。

【0418】なお、アップグレードの態様は、前述したように、

利用制限回数の変更(回数増加)

オンライン回数制限→期間制限へ変更

オンライン回数制限→オンライン回数制限へ変更

オンライン回数制限→買い切りへ変更

のいずれかであり、回数制限の変更の場合は、利用制限回数を新たに設定したアップグレード属性証明書を生成する。また、期間制限へ変更する場合は、期間制限情報

を格納したアップグレード属性証明書を生成する。

【0419】オフライン回数制限として利用制限回数を変更する場合、買い切りへ変更する場合は、アップグレード属性証明書に格納するコンテンツ鍵は、元の属性証明書と同様、サービスプロバイダ管理領域に格納されたSP対応ストレージ秘密鍵：S C. S t o p r i . S P. Kに対応する公開鍵で暗号化したコンテンツ鍵、すなわち、[S C. S t o p u b . S P. K (Kc)]として格納するが、期間制限へ変更、またはオンライン回数制限へ変更する場合は、元の属性証明書とは異なり、アップグレード属性証明書に格納するコンテンツ鍵は、サービスプロバイダの秘密鍵で暗号化したコンテンツ鍵[S P. S t o . K (Kc)]とする。

【0420】なお、オンライン処理とする場合であって、公開鍵方式ではなく、共通鍵方式の適用を行なっている場合は、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたSP対応ストレージ鍵（共通鍵）によって暗号化したコンテンツ鍵を格納する。なお、サービスプロバイダがこの共通鍵を保有していない場合は、図47のステップ(d3)のセキュリティチップからサービスプロバイダへの属性証明書の送付時に、併せてSP対応ストレージ鍵（共通鍵）を送付する。この場合は、相互認証時に生成したセッション鍵で暗号化して送付する。

【0421】サービスプロバイダは、アップグレード属性証明書を生成すると、これをセキュリティチップに送付する。

【0422】(d6) セキュリティチップ制御部は、サービスプロバイダからのアップグレード属性証明書(A C)を受信すると、属性証明書の検証処理を実行する。検証処理には、格納された権限情報(コンテンツ利用条件)が指定条件と一致するかの確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図20の処理フローと同様のシーケンスに従って実行される。さらに、必要に応じてセキュリティチップの制御部は、属性証明書(A C)内のAC保持者の公開鍵証明書情報を従って、公開鍵証明書の連鎖検証を行なうことが好ましい。なお、この連鎖検証が必須の場合もある。

【0423】(d7) 属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード属性証明書受信確認を送信し、(d8)アップグレード属性証明書をメモリに格納する。

【0424】さらに、セキュリティチップの制御部は、アップグレード属性証明書がオフライン回数制限である場合には、コンテンツの利用時までに前述した利用回数管理データのインポート処理を実行する。利用回数管理データインポート処理の詳細は、先に図37～図41を参照して説明した通りであり、セキュリティチップ内部

に利用可能回数を格納する態様と、外部メモリに利用可能回数を格納し、セキュリティチップにハッシュ値のみを格納する態様がある。

【0425】以上の処理により、ユーザデバイスは、すでに保持する属性証明書に基づいて新たなアップグレード属性証明書を取得し、アップグレード属性証明書に従った利用条件にしたがったコンテンツの利用が可能となる。

【0426】(D) アルバム購入型アップグレード

10 次に、一連のアルバム化されたコンテンツデータ、例えば1枚のCDあるいはDVD等に格納された複数(n)のコンテンツ1～n、あるいは何らかのシリーズ化されたコンテンツ1～nがあり、これらのいくつかを購入済であり、購入済みコンテンツに対応する属性証明書1～属性証明書nの複数をユーザがユーザデバイス内に保持している場合、これらの属性証明書をサービスプロバイダに提示することにより、アルバムを構成する他のコンテンツ、すなわち、コンテンツ2, 4, 6～nのコンテンツを割引価格で一括(アルバム)購入する処理とした20 アップグレード処理について、図48を参照して説明する。

【0427】図48は、左からユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部(上位ソフトウェア)、およびサービスプロバイダの処理を示している。最上段(a)は、属性証明書がセキュリティチップの内部メモリに格納されている場合における属性証明書からのサービスプロバイダID取得処理、(b)は、属性証明書がセキュリティチップの外部メモリ、すなわちユーザデバイス制御部単独の制御でアクセス可能なメモリに格納されている場合における属性証明書からのサービスプロバイダID取得処理を示し、(c)はセキュリティチップとサービスプロバイダの相互認証処理である。これらの処理は、前述の図45の場合と同様であり、説明を省略する。

【0428】相互認証後成立後の処理から説明する。

(d1) ユーザは、ユーザデバイスの付属のブラウザにより表示された属性証明書の権限情報(コンテンツ利用条件)を確認し、属性証明書のアップグレード適用要求と、アップグレード条件をセキュリティチップに対して出力する。この例におけるアップグレード処理対象の属性証明書は、ある複数のコンテンツの集合として識別されるアルバムを構成する一部のコンテンツに対応する1以上の属性証明書である。ユーザの指定するアップグレード条件は、例えば、

アルバムを構成する他の一部コンテンツの購入  
アルバムを構成する他の全コンテンツの購入等の条件である。

【0429】(d2) セキュリティチップ制御部は、ユーザデバイス制御部からの属性証明書(A C)アップグレード適用要求を受信すると、属性証明書の検証処理を

実行する。検証処理には、権限情報（コンテンツ利用条件）の確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図20の処理フローと同様のシーケンスに従って実行される。さらに、必要に応じてセキュリティチップの制御部は、属性証明書（AC）内のAC保持者の公開鍵証明書、さらに、連鎖公開鍵証明書の検証を行ない、ルート認証局（CA）の発行した公開鍵証明書の検証まで実行することが好ましい。なお、この連鎖検証が必須の場合もある。

【0430】(d3) 属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード処理対象の属性証明書を、ユーザにより指定されたアップグレード条件情報をともに送付する。

【0431】(d4) セキュリティチップから属性証明書を受信したサービスプロバイダは、属性証明書の署名検証処理を実行する。また、この際、属性証明書にリンクする公開鍵証明書、およびその上位公開鍵証明書を連鎖的に検証することが好ましい。なお、この連鎖検証が必須の場合もある。これらの検証処理により、属性証明書の正当性が確認されると、(d5)ユーザにより指定されたアップグレード条件情報を基づくアップグレード属性証明書生成処理を実行する。

【0432】アップグレード属性証明書生成処理は、ユーザにより指定されたコンテンツ利用条件を記録した新たな属性証明書、すなわちセキュリティチップから受信した属性証明書と異なるシリアル番号を持つ属性証明書を発行する処理として実行する。なお、この際、新たに発行するアップグレード属性証明書中には、アップグレードのベースとなった属性証明書のシリアルを含む履歴データを格納する。

【0433】なお、アップグレードの態様は、前述したように、

アルバムを構成する他の一部コンテンツの購入  
アルバムを構成する他の全コンテンツの購入  
のいずれかであり、アルバムを構成する他の一部コンテンツの購入の場合は、購入指定の一部コンテンツに対応するアップグレード属性証明書を生成する。また、アルバムを構成する他の全コンテンツの購入の場合は、アルバムを構成する他の全コンテンツに対応するアップグレード属性証明書を生成する。

【0434】なお、この場合の利用条件は、ユーザが予め指定することも可能であり、また、サービスプロバイダが決定する構成としてもよい。ユーザが指定する場合は、図48のステップ(d1)において指定し、(d3)のセキュリティチップからサービスプロバイダへの属性証明書の送付時に、指定条件を併せて送付する。

【0435】サービスプロバイダは、オフライン利用とするアップグレード属性証明書を生成する場合は、サー

ビスプロバイダ管理領域に格納されたSP対応ストレージ秘密鍵：SC. Stopri. SP. Kに対応する公開鍵で暗号化したコンテンツ鍵【SC. Stopub. SP. K (Kc)】を格納し、オンライン利用とするアップグレード属性証明書を生成する場合は、アップグレード属性証明書に格納するコンテンツ鍵は、サービスプロバイダの秘密鍵で暗号化したコンテンツ鍵【SP. St o. K (Kc)】とする。

【0436】なお、オフライン処理とする場合であって、公開鍵方式ではなく、共通鍵方式の適用を行なっている場合は、ユーザデバイスのセキュリティチップのサービスプロバイダ管理領域に格納されたSP対応ストレージ鍵（共通鍵）によって暗号化したコンテンツ鍵を格納する。なお、サービスプロバイダがこの共通鍵を保有していない場合は、図48のステップ(d3)のセキュリティチップからサービスプロバイダへの属性証明書の送付時に、併せてSP対応ストレージ鍵（共通鍵）を送付する。この場合は、相互認証時に生成したセッション鍵で暗号化して送付する。

【0437】サービスプロバイダは、アップグレード属性証明書を生成すると、これをセキュリティチップに送付する。

【0438】(d6) セキュリティチップ制御部は、サービスプロバイダからのアップグレード属性証明書（AC）を受信すると、属性証明書の検証処理を実行する。検証処理には、格納された権限情報（コンテンツ利用条件）が指定条件と一致するかの確認、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図20の処理フローと同様のシーケンスに従って実行される。さらに、必要に応じてセキュリティチップの制御部は、属性証明書（AC）内のAC保持者の公開鍵証明書情報を従って、公開鍵証明書の連鎖検証を行なうことが好ましい。なお、この連鎖検証が必須の場合もある。

【0439】(d7) 属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、サービスプロバイダに対してアップグレード属性証明書受信確認を送信し、(d8)アップグレード属性証明書をメモリに格納する。

【0440】さらに、セキュリティチップの制御部は、アップグレード属性証明書がオフライン回数制限である場合には、コンテンツの利用時までに前述した利用回数管理データのインポート処理を実行する。利用回数管理データインポート処理の詳細は、先に図37～図41を参照して説明した通りであり、セキュリティチップ内部に利用可能回数を格納する態様と、外部メモリに利用可能回数を格納し、セキュリティチップにハッシュ値のみを格納する態様がある。

【0441】以上の処理により、ユーザデバイスは、すでに保持する属性証明書に基づいて新たなアップグレード属性証明書を生成する。

ド属性証明書を取得し、アップクレード属性証明書に従った利用条件にしたがったコンテンツの利用が可能となる。

【0442】[データバックアップおよびリストア処理] ユーザがサービスプロバイダから購入し、セキュリティチップを有するユーザデバイス内の記憶手段に格納した権利情報や、証明書類は、消失の事態に備えてバックアップしておくことが好ましい。バックアップすべき情報には、見られてもいい情報と、セキュアに保持しなければいけない情報がある。見られてもいい情報とは、公開鍵証明書、属性証明書などの証明書類である。セキュアに保持する情報とは、例えばセキュリティチップのサービスプロバイダ管理領域に書き込まれているサービス加入の証拠情報などがある。

【0443】公開鍵証明書、属性証明書などの証明書類については、ユーザが適宜、ハードディスクやフラッシュメモリを搭載したメモリカードなどに複製情報を格納しておくことで十分である。属性証明書にはコンテンツ鍵が格納されているが、オンライン利用の場合には、サービスプロバイダとの接続が必要となり、この際の相互認証時にデバイス（セキュリティチップ）の正当性が確認されるので、コンテンツが不正に利用されることはない。また、オフライン利用の場合でも、コンテンツ鍵を復号するための鍵は、セキュリティチップのサービスプロバイダ管理領域に格納されているので、正当なユーザデバイスのセキュリティチップを保持し、かつ前述したパスワードによるアクセスが許可されたユーザのみが暗号化コンテンツ鍵を復号することが可能となる。従って、属性証明書が第三者に渡ったとしてもコンテンツの不正利用が発生することはない。

【0444】しかし、セキュリティチップ内の秘密情報に関しては、テンポラリのストレージにセキュアに保持しておかねばならない。例えばセキュリティチップのサービスプロバイダ管理領域には、サービスプロバイダとの相互認証に必要なID情報、鍵情報、パスワード等が格納されており、これらは第三者に漏洩することを防止することが必要である。従って外部の記憶媒体（テンポラリのストレージ）にバックアップする際には、これらのバックアップデータは、暗号化しておくことが必要である。

【0445】ユーザが秘密情報をテンポラリのストレージに格納した場合、ストレージメディアの盗難によりデータ漏洩が発生する暗号化では意味がない。また、ユーザデバイスから容易に取り出せる鍵によって復号できる構成とすると、ユーザデバイスから取り出した鍵によって、セキュリティデバイスの複製を生成することが可能となってしまい、ユーザサイドで全く同様のサービスプロバイダ管理領域データを有する第2のセキュリティデバイスを生成することが可能となるおそれがある。また、複製したセキュリティチップを搭載した可搬メディ

アを他のユーザデバイスに装着することで、複数のユーザデバイスで全く同様のサービスを受けることが可能となってしまう。そこで本発明のシステムでは、テンポラリのストレージに秘密情報をバックアップデータとして格納した場合でも、不正な第三者によって復号できない態様とするとともに、ユーザデバイスを保持するユーザ自身もシステムホルダの許可なくリストア等、他のセキュリティチップに格納して使用することのできない構成とし、データの復号、リストアはサポートセンタにおいてのみ実行可能とした。

【0446】すなわち、ユーザデバイス内で確実な情報管理を実行し、データ消失を完全に防ぐことの困難性に鑑み、本発明のシステムにおいては、サポートセンタにおいて、データのバックアップ・サービスを提供し、必要に応じてサポートセンタにおいて、バックアップデータを用いてデータ復旧、すなわちリストア処理を実行する。リストアは、サポートセンターにて行い、テンポラリのストレージからデータを読み出し、ユーザデバイスのセキュリティデバイスに対してインポートする処理として実行する。以下、サポートセンタによるデータバックアップ処理、およびリストア処理について説明する。

【0447】図49に、ユーザデバイス内の秘密情報のバックアップ処理、サポートセンタにおけるリストア処理の概要を説明する図を示す。

【0448】図49において、ユーザデバイス410は、セキュリティチップ411を有し、セキュリティチップには様々なシークレット、すなわち秘密情報が格納されている。秘密情報は、例えばセキュリティチップのサービスプロバイダ管理領域の格納情報であり、サービスプロバイダとの相互認証に必要なID情報、鍵情報、パスワード等である。また、ユーザデバイスのセキュリティチップ外のメモリには、公開鍵証明書、属性証明書が格納される。

【0449】ユーザは、ユーザデバイスの損壊、あるいはデータの消失等に備え、これらの情報をユーザデバイス以外の外部の記憶媒体にバックアップして保存する。例えば公開鍵証明書、属性証明書等を外部のPCのハードディスクに格納したり、フラッシュメモリを備えたカード型記憶媒体などの外部記憶媒体421に格納する。

40 これらは、前述したように、漏洩により、コンテンツの不正利用を発生させるおそれがなく、暗号化されることなく外部の記憶媒体421に格納し、必要に応じてユーザが記憶媒体421からユーザデバイス410にリストアすることが可能である。

【0450】一方、セキュリティチップに格納された秘密情報は、外部の記憶媒体422にバックアップデータとして保存する場合は、ユーザデバイスにおいて一時的な鍵として乱数からバックアップ鍵：K<sub>b</sub>（共通鍵系）を生成し、バックアップ鍵：K<sub>b</sub>によって、各種の秘密情報（Secret Data）を暗号化し、暗号化データ：

〔K<sub>b</sub> (S e c D a t a)〕として記憶媒体422に格納する。さらに、生成したバックアップ鍵：K<sub>b</sub>をサポートセンタの公開鍵：K<sub>p s</sub>によって暗号化した暗号鍵データ〔K<sub>p s</sub> (K<sub>b</sub>)〕を併せて外部記憶媒体422に格納する。秘密情報を外部の記憶媒体422に格納した後、バックアップ鍵：K<sub>b</sub>はユーザデバイスに保持することなく消去する。

【0451】記憶媒体422に格納した暗号化データ：〔K<sub>b</sub> (S e c D a t a)〕は、たとえ記憶媒体422が第三者の手に渡ったとしても、その復号のための鍵であるバックアップ鍵：K<sub>b</sub>が、サポートセンタの公開鍵：K<sub>p s</sub>によって暗号化されており、バックアップ鍵：K<sub>b</sub>を取得するためには、サポートセンタの秘密鍵：K<sub>s s</sub>による復号化処理が必要となるので、第三者による復号は不可能である。また、ユーザデバイスを保持する正当なユーザも復号により第2のセキュリティデバイスを生成することはできない。

【0452】データのリストア（復旧）処理は、ユーザサイト側からサポートセンタ450に対して記憶媒体422を送付することによって実行される。リストア処理は、元のユーザデバイスが損壊した場合は、新たなユーザデバイス430に対して実行される。元のユーザデバイス自体をサポートセンタに送付して、修理された元のユーザデバイスに対してリストアを実行することも可能である。なお、新たなユーザデバイスに対するリストア処理を実行する場合は、元のユーザデバイスを無効化する処理、すなわちリボーカ処理を併せて実行する。このリボーカ処理は、例えばユーザデバイスに対応して発行されている公開鍵証明書をリボケーションリストに登録することによって行われる。リボケーションリストは、不正デバイス、無効化されたデバイス、ユーザ等に対応する公開鍵証明書のリストとして構成されるものである。リボケーションリストは、デバイスとの相互認証時に参照され、リストに記載されたデバイスであると判定されると認証を不成立として、その後のデータ通信を中止することを可能としたものである。

【0453】サポートセンタ450におけるリストア処理は、まず、ユーザサイトから送付された記憶媒体422'に格納されたサポートセンタの公開鍵：K<sub>p s</sub>によって暗号化した暗号鍵データ〔K<sub>p s</sub> (K<sub>b</sub>)〕を取り出して、サポートセンタの秘密鍵：K<sub>s s</sub>によって復号してバックアップ鍵：K<sub>b</sub>を取り出す。その後、取得したバックアップ鍵：K<sub>b</sub>を適用して、バックアップ鍵により暗号化された秘密情報暗号化データ：〔K<sub>b</sub> (S e c D a t a)〕の復号化処理を実行し、復号データ：S e c D a t aをユーザデバイス430のセキュリティチップ内に格納する処理として実行される。具体的なリストア処理シーケンスについては、後述する。

【0454】上述したように、ユーザデバイス内の秘密情報をバックアップデータのリストアをサポートセンタ

のみにおいて実行可能とした構成により、秘密情報の複製利用を防止することが可能となる。

【0455】図50にリストア処理時の手順概要を説明する図を示す。ユーザサイトでは、ユーザが使用しているユーザデバイス470内のセキュリティチップに格納された秘密情報をバックアップストレージメディア471に格納する。前述したように、ユーザデバイスは、バックアップ鍵：K<sub>b</sub>（共通鍵系）を生成し、バックアップ鍵：K<sub>b</sub>によって秘密情報（S e c D a t a）を暗号化したデータ：〔K<sub>b</sub> (S e c D a t a)〕と、バックアップ鍵：K<sub>b</sub>をサポートセンタの公開鍵：K<sub>p s</sub>によって暗号化した暗号鍵データ〔K<sub>p s</sub> (K<sub>b</sub>)〕をバックアップストレージメディア471に格納する。

【0456】ユーザデバイス470が損壊する等の理由により、使用できなくなった場合、ユーザは、バックアップストレージメディア471をサポートセンタ475に送付する。

【0457】サポートセンタ475は、新規のユーザデバイス、あるいは損壊したユーザデバイスを修理した元のユーザデバイスに対して、バックアップストレージメディア471のデータを復号してリストアし、秘密情報をリストアしたユーザデバイス472と、リストアに使用したバックアップストレージメディア471をユーザに返却する。サポートセンタ475は、このリストア処理において、新規デバイスに対してリストア処理を実行し、元のデバイスを使用しない場合には、前述したリボーカションリストへの登録によるリボーカ処理を実行する。またサポートセンタ475は、リストア処理に対する課金を実行してもよい。

【0458】図51を参照して、ユーザサイトで実行するバックアップストレージメディアに対するデータバックアップ処理シーケンスについて説明する。図51は、左からバックアップストレージメディア、ユーザデバイス内のセキュリティチップ制御部、ユーザデバイス制御部（上位ソフトウェア）の処理を示している。まず、

（1）ユーザデバイス制御部は、セキュリティチップ制御部に対してバックアップ処理要求を送信する。これは、ユーザがユーザデバイス側の入力部に対するユーザによるバックアップ処理実行指示に基づいて行われる。

【0459】セキュリティチップの制御部は、バックアップ要求を受信すると、（2）バックアップデータの暗号化に適用するバックアップ鍵（キー）：K<sub>b</sub>を生成する。バックアップ鍵（キー）：K<sub>b</sub>は例えば乱数生成手段によって生成した乱数に基づいて生成するバックアップ専用の一時的な鍵であり、バックアップストレージメディアに対するバックアップ処理の後、セキュリティチップに保持されることなく、消去される。

【0460】セキュリティチップの制御部は、（3）バックアップ鍵（キー）：K<sub>b</sub>の生成後、生成したバックアップ鍵（キー）で、バックアップデータの暗号化を行

ない、暗号化データ：[K<sub>b</sub> (S e c D a t a)]を生成する。データ暗号化が終了すると、さらに、(4)セキュリティチップの制御部は、バックアップ鍵(キー)：K<sub>b</sub>をサポートセンタの公開鍵：K<sub>p s</sub>を用いて暗号化して暗号鍵データ：[K<sub>p s</sub> (K<sub>b</sub>)]を生成する。

【0461】上記処理の後、セキュリティチップの制御部は、(5)暗号化データ：[K<sub>b</sub> (S e c D a t a)]と、暗号鍵データ：[K<sub>p s</sub> (K<sub>b</sub>)]をバックアップストレージメディアに格納する。なお、これらの処理の後、バックアップ鍵(キー)：K<sub>b</sub>は、セキュリティチップから消去される。

【0462】なお、バックアップストレージメディアに暗号化データ：[K<sub>b</sub> (S e c D a t a)]と、暗号鍵データ：[K<sub>p s</sub> (K<sub>b</sub>)]を格納することなく、これらのデータを直接サポートセンタに送信し、サポートセンタ内の記憶手段にユーザデバイスID、またはセキュリティチップIDに対応させてバックアップデータを保存する構成としてもよい。このような構成とした場合は、バックアップデータに基づくリストア処理は、ユーザデバイス(セキュリティチップ)側からサポートセンタに対する通信ネットワークを介したリクエストに応じて実行可能となり、バックアップストレージメディアを送付することなく、リストア処理を実行することが可能となる。

【0463】次に、図52を参照して、サポートセンタで実行するバックアップストレージメディアからのバックアップデータの取得処理について説明する。サポートセンタでは、まず、ユーザサイトから送付されたバックアップストレージメディアに格納されたデータを読み出す。読み出しデータは、バックアップ鍵(キー)：K<sub>b</sub>で暗号化されたバックアップデータ：[K<sub>b</sub> (S e c D a t a)]と、バックアップ鍵(キー)：K<sub>b</sub>をサポートセンタの公開鍵：K<sub>p s</sub>を用いて暗号化した暗号鍵データ：[K<sub>p s</sub> (K<sub>b</sub>)]である。なお、前述したように、サポートセンタ内の記憶手段にユーザデバイスID、またはセキュリティチップIDに対応させてバックアップデータを保存した構成とした場合は、サポートセンタは、ユーザサイトからのリストア処理リクエストに基づいて、記憶手段からこれらのデータの読み出しを行なう。

【0464】サポートセンタは、データの読み出しの後、まずサポートセンタの公開鍵：K<sub>p s</sub>で暗号化したバックアップ鍵(キー)：K<sub>b</sub>データ：[K<sub>p s</sub> (K<sub>b</sub>)]を、サポートセンタの公開鍵に対応する秘密鍵：K<sub>s s</sub>で復号化処理を実行し、バックアップ鍵(キー)：K<sub>b</sub>を取り出す。さらに、バックアップ鍵(キー)：K<sub>b</sub>で暗号化されたバックアップデータ：[K<sub>b</sub> (S e c D a t a)]を取り出したバックアップ鍵(キー)：K<sub>b</sub>を適用して復号化処理を実行し、バック

アップデータ：S e c D a t aを取り出す。

【0465】次に、図53を参照して、サポートセンタで実行するリストア処理のシーケンスについて説明する。図53は、左から、リストア処理によりデータを格納する新たなユーザデバイスのセキュリティチップ制御部、およびユーザデバイス制御部、サポートセンタサーバ、さらに、属性証明書発行者である属性証明書認証局(AA：Attribute Certificate Authority)の処理を示している。なお、属性証明書発行局は、属性証明書を発行する機関であり、例えばサービスプロバイダ内に構成される。ここで属性証明書発行局は、ユーザデバイスのセキュリティチップ内のメモリにサービスプロバイダ管理領域を生成するための属性証明書である。

【0466】前述したように、サービスプロバイダ管理領域生成用の属性証明書は、サービスプロバイダがユーザデバイスのセキュリティチップ内のメモリにサービスプロバイダ毎の管理領域を登録設定することを目的として発行される属性証明書であり、属性情報フィールドには、サービスプロバイダ識別子(ID)、サービスプロバイダ・ネーム、処理様式：メモリ領域確保、領域サイズ：メモリ領域のサイズ等が記録される。

【0467】図53の処理シーケンスについて説明する。まず、(1)ユーザデバイス制御部からセキュリティチップ制御部に対してリストア処理要求が送出される。これは、サポートセンタのオペレータによってユーザデバイス側の入力部に対して実行するリストア処理実行指示に基づいて行われる。

【0468】セキュリティチップ制御部は、(2)ユーザデバイス制御部からリストア処理要求を受信すると、(3)セキュリティチップとサービスプロバイダ間の相互認証処理を実行する。この相互認証処理は、先に説明した図16のTLS1.0処理または、その他の方式、例えば公開鍵方式による相互認証処理として実行される。この相互認証処理においては、相互の公開鍵証明書の検証がなされ、必要に応じてルート認証局(CA)までの公開鍵証明書が連鎖的に検証される。この認証処理において、セキュリティチップと、サポートセンタはセッション鍵(K<sub>s e s</sub>)を共有する。相互認証が成立すると、次に、(4)セキュリティチップ制御部は、サポートセンタに対してリストア処理要求を送信する。

【0469】サポートセンタは、セキュリティチップからのリストア処理要求を受信すると、(5)バックアップデータの検索処理を行なう。これは、サポートセンタが、ユーザサイトからバックアップデータを受領済みであるか否かの確認として実行される。

【0470】サポートセンタは、次に、(6)メモリ領域確保用属性証明書(AC)の発行要求を属性証明書発行局(者である)に対して送信する。(7)属性証明書(AC)の発行要求を受信した属性証明書発行者である属性証明書認証局(AA)は、メモリ領域確保用属性証

明書(AC)を生成する。なお、属性証明書(AC)は、予め属性証明書認証局(AA)から発行を受けておいてよい。

【0471】メモリ領域確保用属性証明書は、属性情報フィールドに、サービスプロバイダ識別子(ID)、サービスプロバイダ・ネーム、処理態様：メモリ領域確保、領域サイズ：メモリ領域のサイズ等が記録されたものであり、例えば各サービスプロバイダの管理の下に発行される。従って、リストア処理が1つのサービスプロバイダ管理領域内のデータについてのみ実行される場合は、1つのメモリ領域確保用属性証明書によりセキュリティチップ制御部内のメモリに1つのサービスプロバイダ管理領域が設定され、データのリストアが実行されるが、複数のサービスプロバイダ管理領域内のデータについてリストアを実行する場合は、複数のメモリ領域確保用属性証明書の発行を受けて、セキュリティチップ制御部内のメモリに複数のサービスプロバイダ管理領域を設定した上で、各利用域についてデータ格納を行なうことになる。

【0472】(8) 属性証明書発行者である属性証明書認証局(AA)は、生成したメモリ領域確保用属性証明書(AC)をサポートセンタサーバに送信する。サポートセンタは、属性証明書発行者である属性証明書認証局(AA)からメモリ領域確保用属性証明書(AC)を受信すると、(9) 属性証明書、およびバックアップデータをセキュリティチップ制御部に送信する。バックアップデータは、メモリ領域確保用属性証明書(AC)によって、セキュリティチップのメモリに確保されるサービスプロバイダ管理領域に格納するデータであり、例えば、サービスプロバイダ(SP)対応秘密鍵、サービスプロバイダ(SP)対応ストレージ秘密鍵、外部管理情報のハッシュ値、利用回数管理データ、認証情報、ユーザ情報等の各データである。

【0473】(10) セキュリティチップ制御部は、サポートセンタサーバからのメモリ領域確保用属性証明書(AC)を受信すると、属性証明書の検証処理を実行する。検証処理には、フォーマット確認、署名検証処理が含まれる。署名検証処理は、例えば先に説明した図20の処理フローと同様のシーケンスに従って実行される。

【0474】さらに、必要に応じてセキュリティチップの制御部は、属性証明書(AC)内のAC保持者の公開鍵証明書情報を従ってリンクする公開鍵証明書を取得して、公開鍵証明書の検証を行なうことが好ましい。例えば属性証明書(AC)の発行者の信頼度が不確かである場合には、属性証明書(AC)の発行者の公開鍵証明書の検証を行なうことによって、認証局の公開鍵証明書を正当に有しているか否かの判定が可能となる。なお、公開鍵証明書が前述したように階層構成をなしている場合は、経路を上位に辿って連鎖的な検証を行ない、ルート認証局(CA)の発行した公開鍵証明書の検証まで実行

することが好ましい。なお、この連鎖検証が必須の場合もある。

【0475】(11) 属性証明書の検証により、属性証明書の改竄なしの判定が得られると、セキュリティチップの制御部は、メモリ領域確保用属性証明書(AC)に記録された条件に従って、セキュリティチップ内のメモリにサービスプロバイダ管理領域を設定する。(12) さらに、セキュリティチップの制御部は、メモリに設定されたサービスプロバイダ管理領域内にサポートセンタサーバから受信したバックアップデータを格納する。

【0476】以上の処理により、ユーザデバイスのセキュリティチップのメモリに、メモリ領域確保用属性証明書に記録された条件に従ってサービスプロバイダ管理領域が確保され、確保されたサービスプロバイダ管理領域にバックアップデータが格納される。なお、複数のサービスプロバイダ管理領域に対応するバックアップデータのリストアを行なう場合は、複数のメモリ領域確保用属性証明書の発行に基づいて同様の処理を繰り返し実行する。

【0477】なお、上述の処理シーケンスの後、あるいはその途中において、サポートセンタは、廃棄対象となる元のユーザデバイスのリポート処理を実行する。さらに、リストアを要求してきたユーザに対する課金処理を実行してもよい。

【0478】[各エンティティの構成] 次に、上述したコンテンツ利用管理システムを構成する各エンティティの構成例について図を参照しながら、説明する。まずサービスプロバイダからのコンテンツを受領するサービス受領デバイスとしてのユーザデバイスの構成例を図54を参照して説明する。

【0479】ユーザデバイスはデータ処理、制御を実行するCPU、サービスプロバイダ他と通信可能な通信手段を備えたPC等のデータ処理手段によって実現することができる。図54にデバイスの構成例を示す。なお、図54に示すデバイス構成例は1つの例であり、デバイスは、ここに示すすべての機能を必ずしも備えることが要求されるものではない。図54に示すCPU(Central processing Unit)501は、各種アプリケーションプログラムや、OS(Operating System)を実行するプロセッサである。ROM(Read-Only-Memory)502は、CPU501が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。RAM(Random Access Memory)503は、CPU501の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。

【0480】HDD504はハードディスクの制御を実行し、ハードディスクに対する各種データ、プログラムの格納処理および読み出し処理を実行する。セキュリティチップ512は、前述したように耐タンパ構造を持つ

構成であり、暗号処理に必要な鍵データ、アクセス許可書の格納領域としてのメモリ、制御部を有する。

【0481】バス510はPCI(Peripheral Component Interface)バス等により構成され、各モジュール、入出力インターフェース511を介した各入手力装置とのデータ転送を可能にしている。

【0482】入力部505は、例えばキーボード、ポインティングデバイス等によって構成され、CPU501に各種のコマンド、データを入力するためにユーザにより操作される。出力部506は、例えばCRT、液晶ディスプレイ等であり、各種情報をテキストまたはイメージ等により表示する。

【0483】通信部507はデバイスの接続したエンティティ、例えばサービスプロバイダ等との通信処理を実行し、CPU501の制御の下に、各記憶部から供給されたデータ、あるいはCPU501によって処理されたデータ、暗号化されたデータ等を送信したり、他エンティティからのデータを受信する処理を実行する。

【0484】ドライブ508は、フロッピー(登録商標)ディスク、CD-ROM(Compact Disc Read Only Memory)、MO(Magneto optical)ディスク、DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体509の記録再生を実行するドライブであり、各リムーバブル記録媒体509からのプログラムまたはデータ再生、リムーバブル記録媒体509に対するプログラムまたはデータ格納を実行する。

【0485】各記憶媒体に記録されたプログラムまたはデータを読み出してCPU501において実行または処理を行なう場合は、読み出したプログラム、データはインターフェース511、バス510を介して例えば接続されているRAM503に供給される。

【0486】前述の説明内に含まれるユーザデバイスにおける処理を実行するためのプログラムは例えばROM502に格納されてCPU501によって処理されるか、あるいはハードディスクに格納されHDD504を介してCPU501に供給されて実行される。

【0487】次に、本発明のシステムの構成エンティティであるサービスプロバイダ、サポートセンタ、コンテンツクリエータ、属性証明書発行局等の各エンティティを構成するデータ処理装置の構成例について説明する。これらのエンティティは例えば図55に構成によって実現することができる。なお、図55に示すデータ処理装置構成例は1つの例であり、各エンティティは、ここに示すすべての機能を必ずしも備えることが要求されるものではない。

【0488】図55に示すCPU(Central processing unit)601は、各種アプリケーションプログラムや、OS(Operating System)602を実際に実行する。ROM(Read-Only-Memory)602は、CPU601が実行するプログラム、あるいは演算パラメータとしての固定デ

ータを格納する。RAM(Random Access Memory)603は、CPU601の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。HDD604はハードディスクの制御を実行し、ハードディスクに対する各種データ、プログラムの格納処理および読み出し処理を実行する。暗号処理手段605は、送信データの暗号処理、復号化処理等を実行する。なお、ここでは、暗号処理手段を個別モジュールとした例を示したが、このような独立した暗号処理モジュールを設けず、例えば暗号処理プログラムをROM602に格納し、CPU601がROM格納プログラムを読み出して実行するように構成してもよい。

【0489】ドライブ606は、フロッピーディスク、CD-ROM(Compact Disc Read Only Memory)、MO(Magneto optical)ディスク、DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体607の記録再生を実行するドライブであり、各リムーバブル記録媒体607からのプログラムまたはデータ再生、リムーバブル記録媒体607に対するプログラムまたはデータ格納を実行する。各記憶媒体に記録されたプログラムまたはデータを読み出してCPU601において実行または処理を行なう場合は、読み出したプログラム、データはバス610を介して例えば接続されているRAM603、通信部608、通信部609に供給される。

【0490】通信部608、通信部609は、それぞれ異なるエンティティを通信相手として通信する処理を想定して複数の通信部を設けた例を示している。例えばサービスプロバイダであれば、一方はユーザデバイスとの通信、他方はコンテンツクリエータとの通信処理に使用される。各通信部を介して通信相手との相互認証、暗号化データの送受信処理等が実行される。

【0491】前述した説明内に含まれるサービスプロバイダ、サポートセンタ、コンテンツクリエータ、属性証明書発行局を構成するデータ処理装置における各処理を実行するためのプログラムは例えばROM602に格納されてCPU601によって処理されるか、あるいはハードディスクに格納されHDD604を介してCPU601に供給されて実行される。

【0492】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲を参酌すべきである。

【0493】なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフト

ウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることができる。

【0494】例えば、プログラムは記録媒体としてのハードディスクやROM(Read OnlyMemory)に予め記録しておくことができる。あるいは、プログラムはフロッピーディスク、CD-ROM(Compact Disc Read Only Memory), MO(Magneto optical)ディスク、DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納(記録)しておくことができる。このようリムーバブル記録媒体は、いわゆるパッケージソフトウェアとして提供することができる。

【0495】なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、LAN(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

【0496】なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的あるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

#### 【0497】

【発明の効果】以上、説明したように、本発明のバックアップデータ管理システム、バックアップデータ管理方法、および情報処理装置、並びにコンピュータ・プログラムによれば、情報処理装置において、バックアップ対象データをバックアップ鍵で暗号化した暗号化バックアップデータを生成するとともに、バックアップ鍵を外部エンティティであるサポートセンタの公開鍵を用いて暗号化した暗号化鍵データを生成し、生成データをバックアップ用メディアに格納、またはサポートセンタに送信する構成としたので、第三者にバックアップデータを格納したメディアが渡ったとしても復号される恐れがなく、ユーザデバイスにおけるバックアップデータ管理の負担が軽減され、データの高度なセキュリティの下での管理が容易となる。

【0498】また、本発明のバックアップデータ管理システム、バックアップデータ管理方法、および情報処理装置、並びにコンピュータ・プログラムによれば、サポートセンタにおけるバックアップデータのリストア処理は、メモリ領域確保用属性証明書に従って情報処理装置

のメモリ内に区分領域を設定し、設定した区分領域にバックアップデータを格納する処理として実行する構成であるので、属性証明書の検証により、正当性の立証された属性証明書に基づいて、メモリ領域が設定され、データのリストアが実行されるので、不正なデータリストアを防止することが可能となる。

#### 【図面の簡単な説明】

【図1】本発明のコンテンツ利用管理システム構成の概要を説明する図である。

10 【図2】本発明のコンテンツ利用管理システムにおいて適用可能な公開鍵証明書のフォーマットを示す図である。

【図3】本発明のコンテンツ利用管理システムにおいて適用可能な公開鍵証明書のフォーマットを示す図である。

【図4】本発明のコンテンツ利用管理システムにおいて適用可能な公開鍵証明書のフォーマットを示す図である。

20 【図5】本発明のコンテンツ利用管理システムにおいて適用可能な権限情報証明書としての属性証明書のフォーマットを示す図である。

【図6】ユーザデバイスにおけるセキュリティチップの構成を示す構成図である。

【図7】ユーザデバイス内での処理対象となる主なデータを示す図である。

【図8】認証情報(パスワード)の初期登録処理シーケンスを示す図である。

【図9】認証情報(パスワード)の変更処理シーケンスを示す図である。

30 【図10】認証情報(パスワード)の変更処理シーケンスを示す図である。

【図11】認証情報(パスワード)とマスタパスワードとの対応について説明する図である。

【図12】マスタパスワードの配布処理について説明する図である。

【図13】マスタパスワードの再発行処理シーケンスを示す図である。

【図14】マスタパスワードの算出処理を示すフロー図である。

40 【図15】属性証明書(A.C.)発行、コンテンツ受信処理シーケンスを示す図である。

【図16】相互認証処理の例であるTLS1.0ハンドシェイクプロトコルのシーケンスを示す図である。

【図17】データ改竄検証に適用するMACの生成処理を説明する図である。

【図18】属性証明書(A.C.)の発行処理シーケンスを示す図である。

50 【図19】署名生成処理の例であるECDSA署名生成手順を説明するフロー図である。

【図20】署名検証処理の例であるECDSA署名検証

手順を説明するフロー図である。

【図21】公開鍵証明書(PKC)と属性証明書(AC)との関連付けについて説明する図である。

【図22】公開鍵証明書(PKC)の検証処理フローを示す図である。

【図23】属性証明書(AC)の検証処理フロー(例1)を示す図である。

【図24】属性証明書(AC)の検証処理フロー(例2)を示す図である。

【図25】属性証明書(AC)を利用したコンテンツ利用処理(オンライン)を説明するシーケンス図である。

【図26】属性証明書(AC)を利用したコンテンツ利用処理(オンライン)を説明するシーケンス図である。

【図27】グローバル共通鍵によるコンテンツ鍵の暗号化データを格納した属性証明書(AC)を利用したコンテンツ利用処理(オンライン)を説明する図である。

【図28】グローバル共通鍵の更新処理を説明するシーケンス図である。

【図29】グローバル共通鍵の更新処理を説明するシーケンス図である。

【図30】デコーダを用いた復号化処理について説明する図である。

【図31】デコーダを用いた復号化処理シーケンスについて説明する図である。

【図32】デコーダを用いた復号化処理フローについて説明する図である。

【図33】ユーザデバイス側における属性証明書(AC)の適用処理を説明するフロー図である。

【図34】属性証明書(AC)を利用したオンライン期間制限コンテンツの利用処理を説明するシーケンス図である。

【図35】属性証明書(AC)を利用したオンライン回数制限コンテンツの利用処理を説明するシーケンス図である。

【図36】属性証明書(AC)を利用したオンライン買い切りコンテンツの利用処理を説明するシーケンス図である。

【図37】オンライン回数制限コンテンツに対応する利用回数管理データのインポート処理を説明する図である。

【図38】オンライン回数制限コンテンツに対応する利用回数管理データのデータ構成例を示す図である。

【図39】オンライン回数制限コンテンツに対応する利用回数管理データのインポート処理を説明するフロー図である。

【図40】オンライン回数制限コンテンツに対応するハッシュ値管理型の利用回数管理データのインポート処理を説明する図である。

【図41】オンライン回数制限コンテンツに対応するハッシュ値管理型の利用回数管理データのインポート処理

を説明するフロー図である。

【図42】オンライン回数制限コンテンツの属性証明書を適用したコンテンツ利用処理を説明する図である。

【図43】オンライン回数制限コンテンツに対応する回数管理データの更新処理を説明する図である。

【図44】オンライン回数制限コンテンツに対応するハッシュ値管理型の回数管理データの更新処理を説明する図である。

【図45】オンライン期間制限属性証明書をベースとして適用したアップグレード処理を説明する図である。

【図46】オンライン回数制限属性証明書をベースとして適用したアップグレード処理を説明する図である。

【図47】オンライン回数制限属性証明書をベースとして適用したアップグレード処理を説明する図である。

【図48】アルバム購入型のアップグレード処理を説明する図である。

【図49】サポートセンタによるデータリストア処理の概要を説明する図である。

【図50】サポートセンタによるデータリストア処理の処理シーケンス概要を説明する図である。

【図51】ユーザデバイス側で実行するデータバックアップ処理シーケンスを説明する図である。

【図52】サポートセンタによるバックアップデータ読み出し処理の概要を説明する図である。

【図53】サポートセンタによるデータリストア処理シーケンスを説明する図である。

【図54】ユーザデバイスの構成例を示す図である。

【図55】サービスプロバイダ、サポートセンタ、コンテンツクリエータ等の各エンティティの構成例を示す図である。

#### 【符号の説明】

101 ユーザデバイス

102 サービスプロバイダ

103 コンテンツクリエータ

104 ユーザデバイス製造者

105 サポートセンタ

106 認証局

110 属性証明書

200 ユーザデバイス

40 201 C P U (Central processing Unit)

202 インタフェース

203 R O M (Read-Only-Memory)

204 R A M (Random Access Memory)

205 暗号処理部

206 メモリ部

210 セキュリティチップ

221 ユーザデバイス側制御部

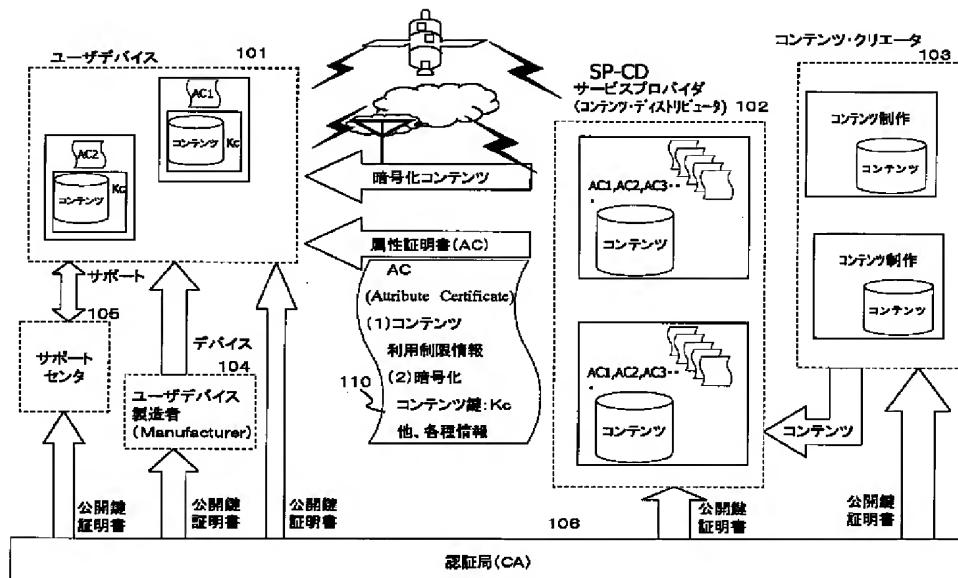
222 外部メモリ部

280 デコーダ

50 301 システムホルダ

3 0 2	サービスプロバイダ	* 5 0 5	入力部
3 0 3	コンテンツクリエータ	5 0 6	出力部
3 0 4	ユーザデバイス	5 0 7	通信部
4 1 0	ユーザデバイス	5 0 8	ドライブ
4 1 1	セキュリティチップ	5 0 9	リムーバブル記録媒体
4 2 1	記憶手段	5 1 0	バス
4 2 2	ストレージメディア	5 1 1	入出力インターフェース
4 3 0	ユーザデバイス	5 1 2	セキュリティチップ
4 5 0	サポートセンタ	6 0 1	C P U (Central processing Unit)
4 7 0	ユーザデバイス	10 6 0 2	R O M (Read-Only-Memory)
4 7 1	ストレージメディア	6 0 3	R A M (Random Access Memory)
4 7 2	ユーザデバイス	6 0 4	H D D
4 7 5	サポートセンタ	6 0 5	暗号処理手段
5 0 1	C P U (Central processing Unit)	6 0 6	ドライブ
5 0 2	R O M (Read-Only-Memory)	6 0 7	リムーバブル記録媒体
5 0 3	R A M (Random Access Memory)	6 0 8 , 6 0 9	通信部
5 0 4	H D D	*	バス

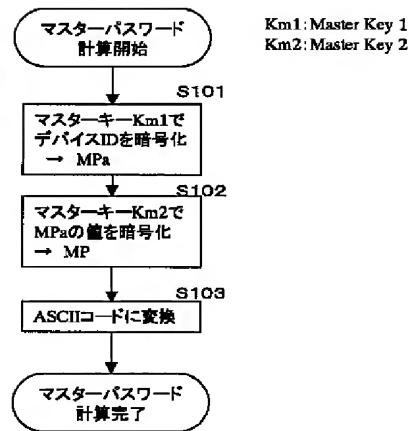
【図1】



【図2】

Version		
V-1	version	証明書のフォーマットのバージョン
	serialNumber	証明書発行者によって割り当てられる証明書番号
	signature	証明書の署名アルゴリズム
	issuer	証明書発行者名(Distinguished Name形式)
	validity notBefore notAfter	証明書の有効期限 開始日時 終了日時
	subject	証明書所有者名
	subjectPublicKeyInfo algorithm subjectPublicKey	証明書所有者の公開鍵情報 鍵のアルゴリズム 鍵

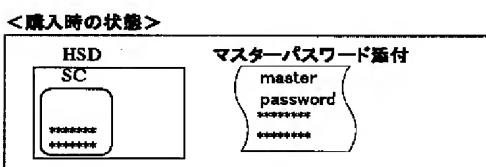
【図14】



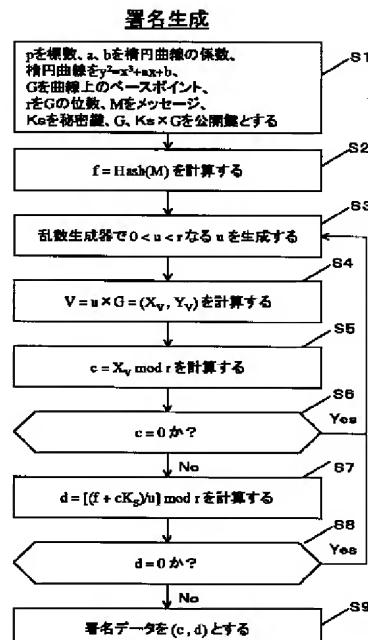
【図3】

V-3	authorityKeyIdentifier keyIdentifier authorityCertIssuer authorityCertSerialNumber	署名検証に用いる証明書発行者の識別子 識別子 機関証明書発行者名(General Name形式) 機関証明書シリアルナンバー
	subjectKeyIdentifier keyIdentifier	複数の鍵の中から目的の鍵を明確に識別
	key usage (0)digitalSignature (1)nonRepudiation (2)keyEncipherment (3)dataEncipherment (4)keyAgreement (5)keyCertSign (6)x509Sign	鍵の使用目的を指定 (0)デジタル署名用 (1)否認防止用 (2)鍵の暗号化用 (3)メッセージの暗号化用 (4)共通鍵配達用 (5)認証の署名確認用 (6)失効リストの署名確認用
	privateKeyUsagePeriod notBefore notAfter	証明書中の公開鍵に対応する秘密鍵の有効期限
	certificatePolicies policyIdentifier policyQualifiers	証明書発行者が承認した証明書ポリシー ポリシーID(ISO/IEC9834-1準拠) 認証基準
	policyMappings issuerDomainPolicy subjectDomainPolicy	認証バス中のポリシーの関係を制限(CA証明書にのみ必要)

【図12】



【図19】



署名生成(IEEE P1363/D13)

【図4】

V-3	subjectAltName	証明書所有者の別名(GN形式)
	issuerAltName	証明書発行者の別名(GN形式)
	subjectDirectoryAttributes	証明書所有者のために必要とされるディレクトリの属性
	basicConstraints cA pathLenConstraint	証明対象の公開鍵が認証局の署名用か、証明書所有者のものかを区別
	nameConstraints permittedSubtrees base minimum maximum ExcludedSubtrees	発行者が発行する証明書の名前を制限
	policyConstraints requireExplicitPolicy InhibitPolicyMapping	認証パス中のポリシーの関係を制限
	cRLDistributionPoints	証明書所有者が証明書を利用する際に、証明書が失効していないかどうかを確認するための失効リストの参照点を記述
	signatureAlgorithm	証明書への署名付けに用いるアルゴリズム
	signatureValue	証明書発行者の秘密鍵による署名

【図5】

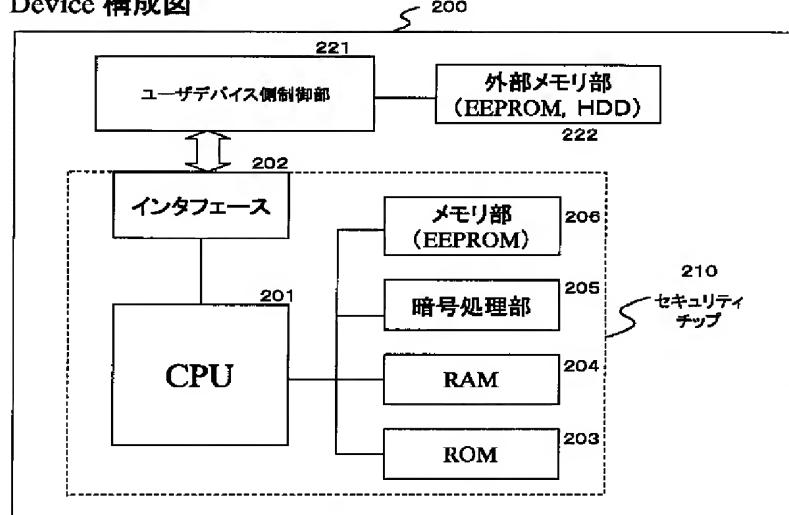
<b>属性証明書 (AC:Attribute Certificate)</b>	
証明書のバージョン番号	
AC保持者の公開鍵証明書情報	
属性証明書発行者の名前	
署名アルゴリズム識別子	
証明書のシリアル番号	
証明書の有効期限	
属性情報フィールド (1)メモリ領域確保、削除関連情報 (2)コンテンツ利用条件関連情報 暗号化コンテンツ鍵、他	
署名アルゴリズム	
属性証明書発行者署名	

【図7】

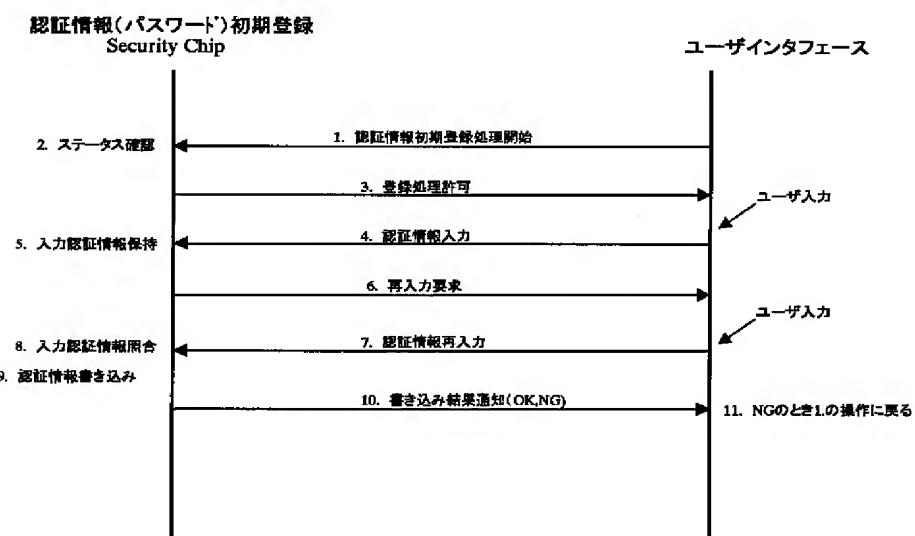
データ種別	データ内容
公開鍵証明書	・ルート認証局公開鍵証明書 ・サービスプロバイダ公開鍵証明書 ・サポートセンタ公開鍵証明書
属性証明書	・アプリケーション(コンテンツ)利用管理用属性証明書 ・SP用メモリ領域管理用属性証明書
鍵データ	・公開鍵、秘密鍵ペア ・ストレージ鍵 (デバイス対応ストレージ鍵:グローバル共通鍵) (サービスプロバイダ対応ストレージ鍵) ・乱数生成用鍵、・相互認証用鍵
識別情報	・デバイスID ・サービスプロバイダID ・ユーザID ・アプリケーションID
その他	・認証情報 ・乱数シード(Seed) ・コンテンツ利用回数情報

【図6】

Device構成図



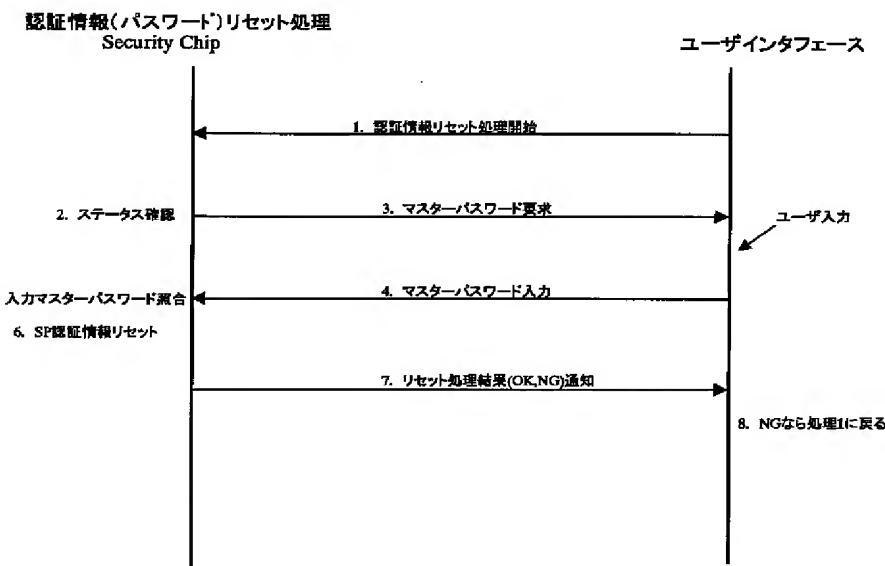
【図8】



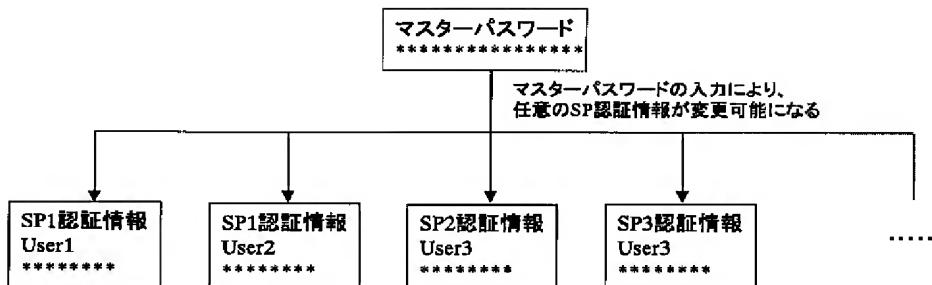
【図9】



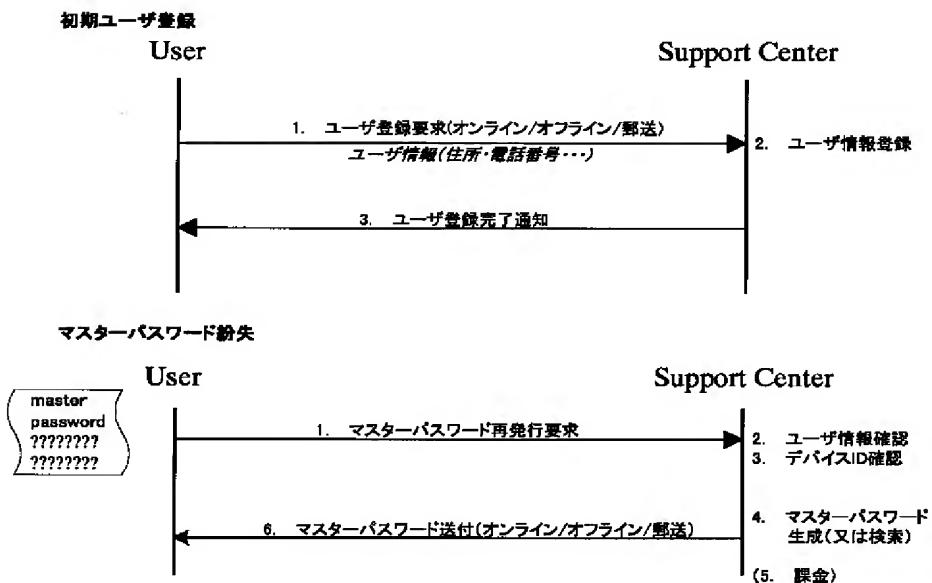
【図10】



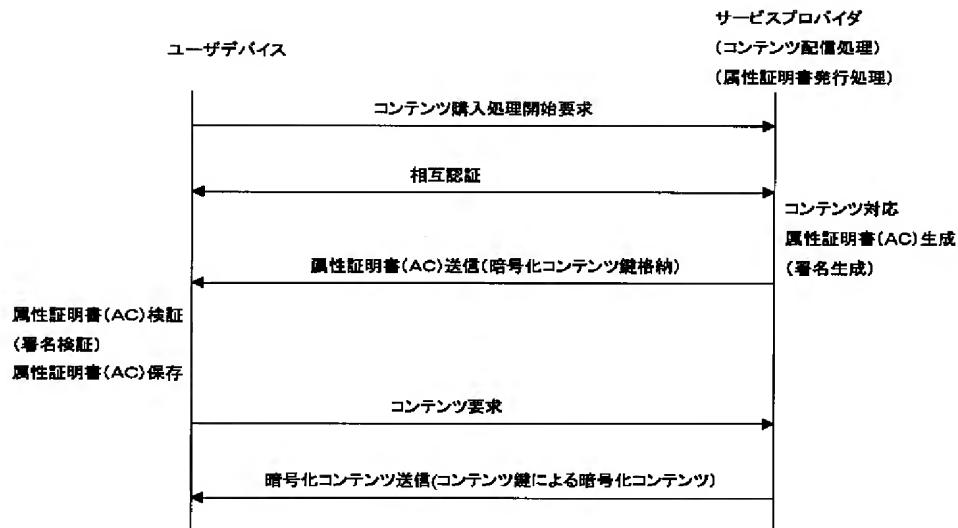
【図11】



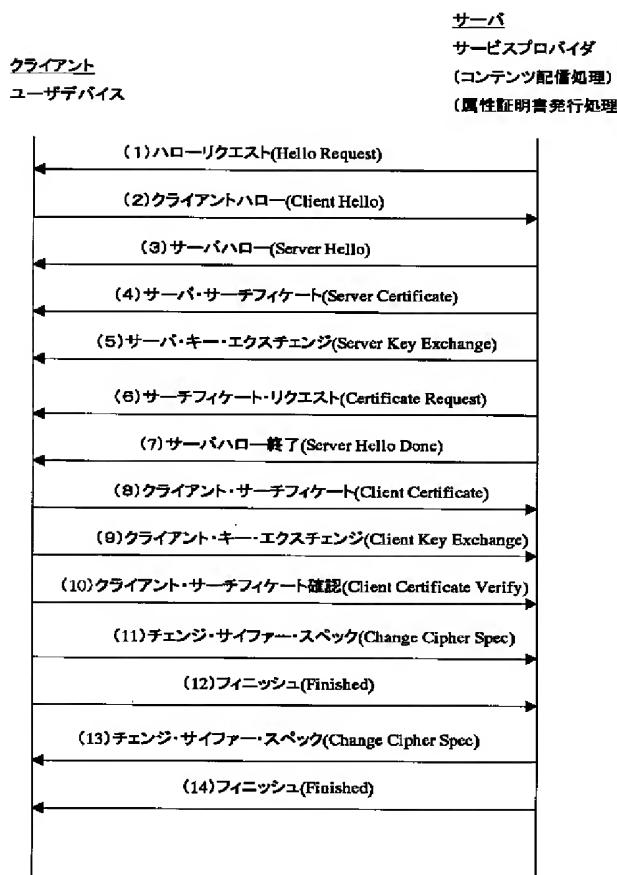
【図13】



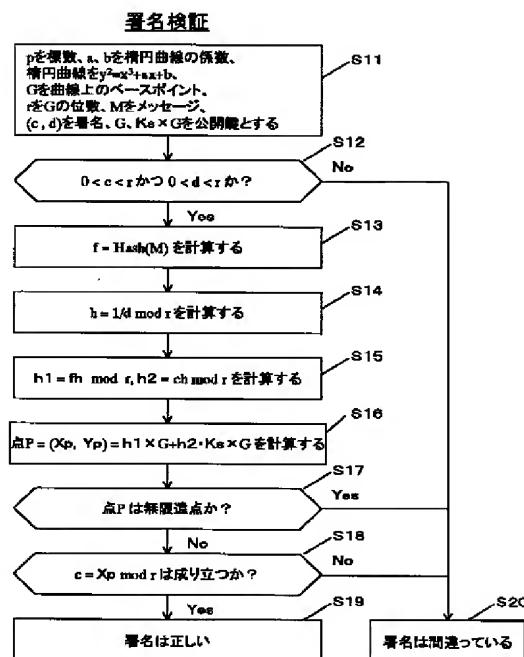
【図15】



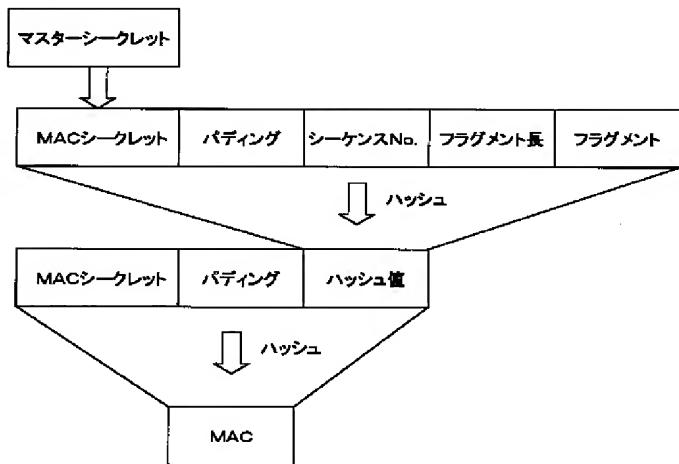
【図16】



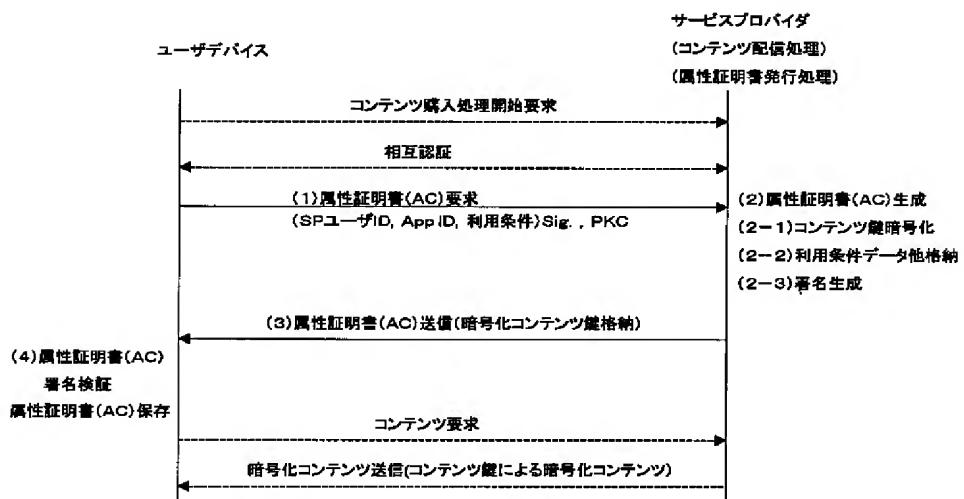
【図20】



【図17】

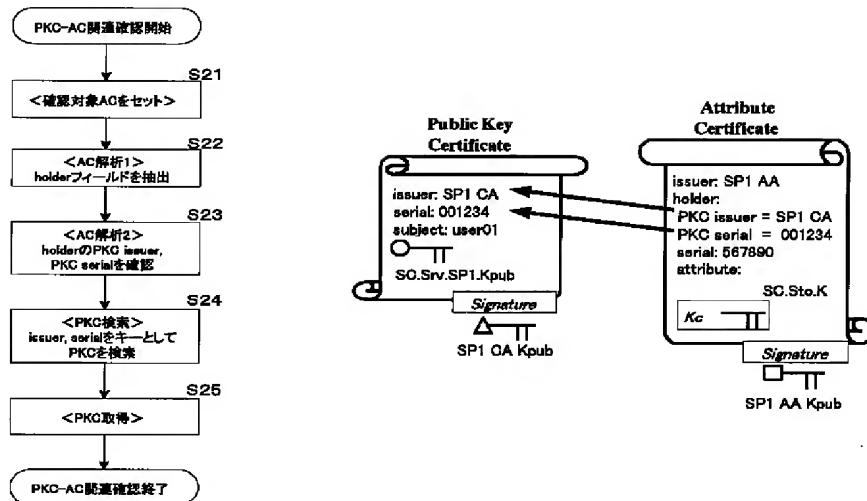


【図18】

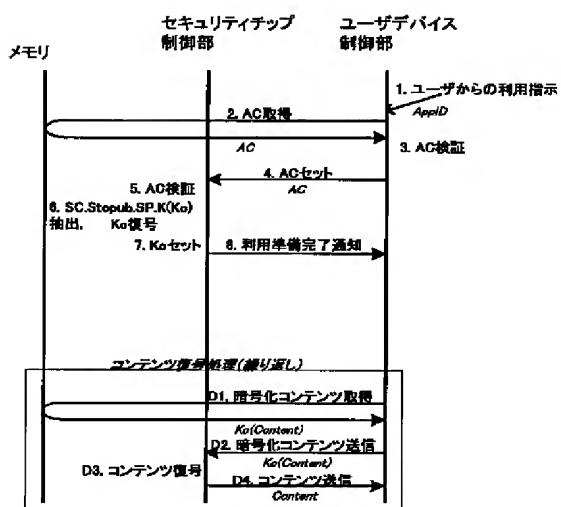


【図21】

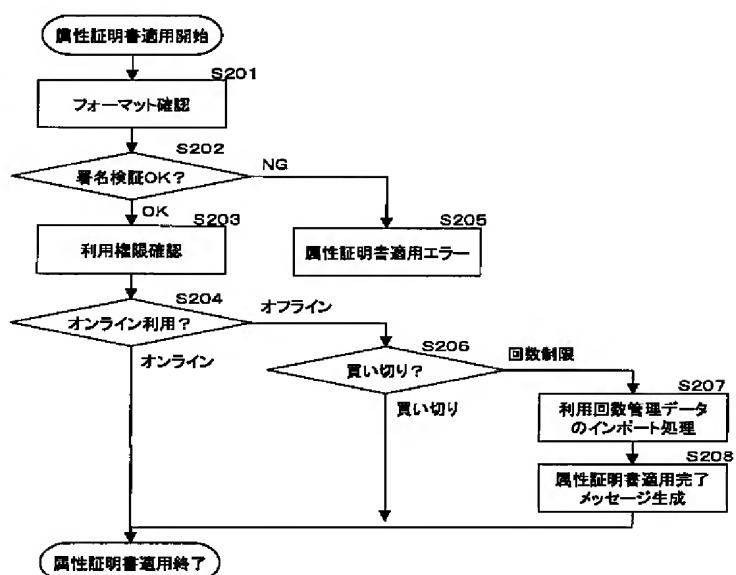
## PKCとACの関連づけ



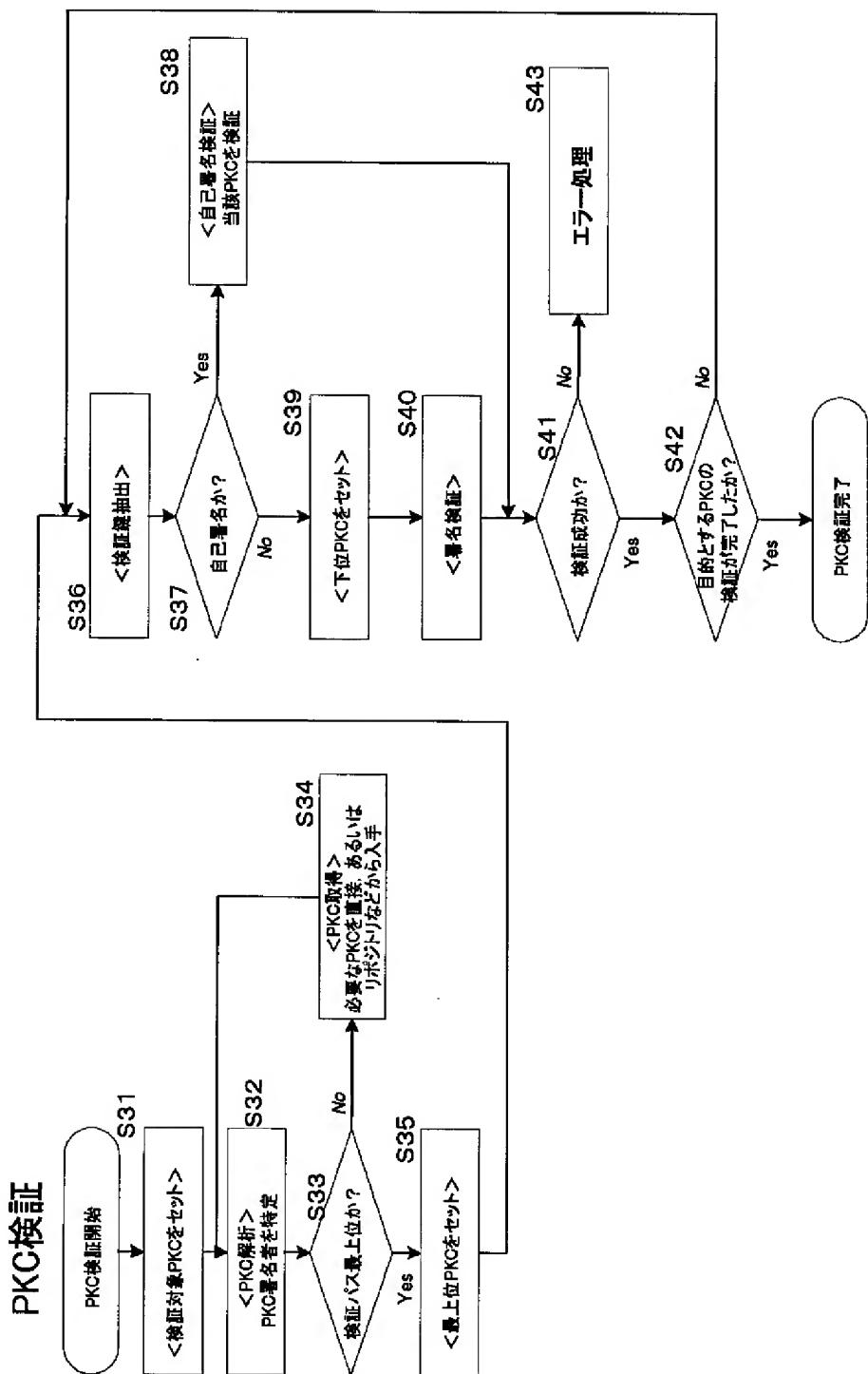
【図25】



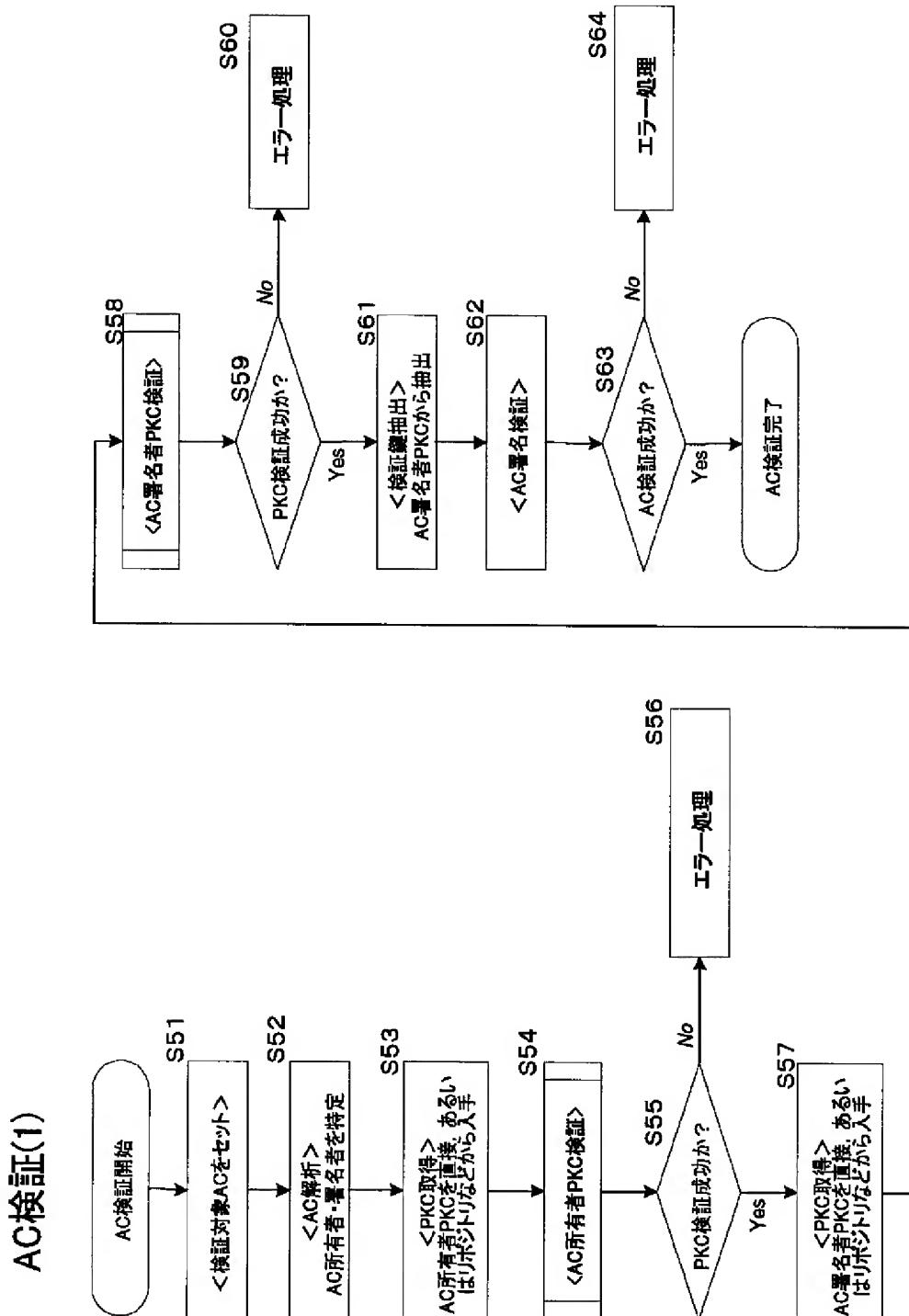
【図33】



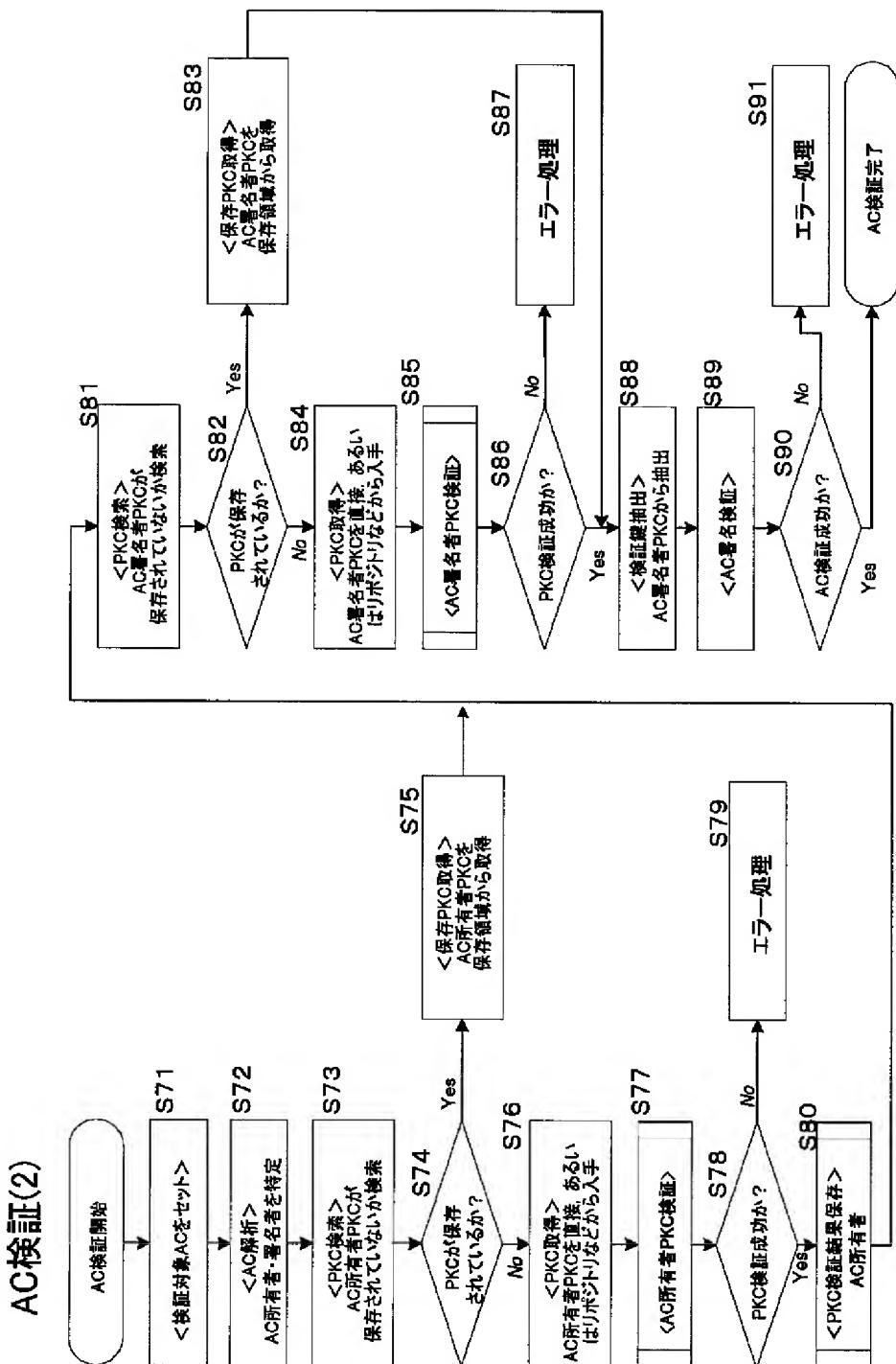
【図22】



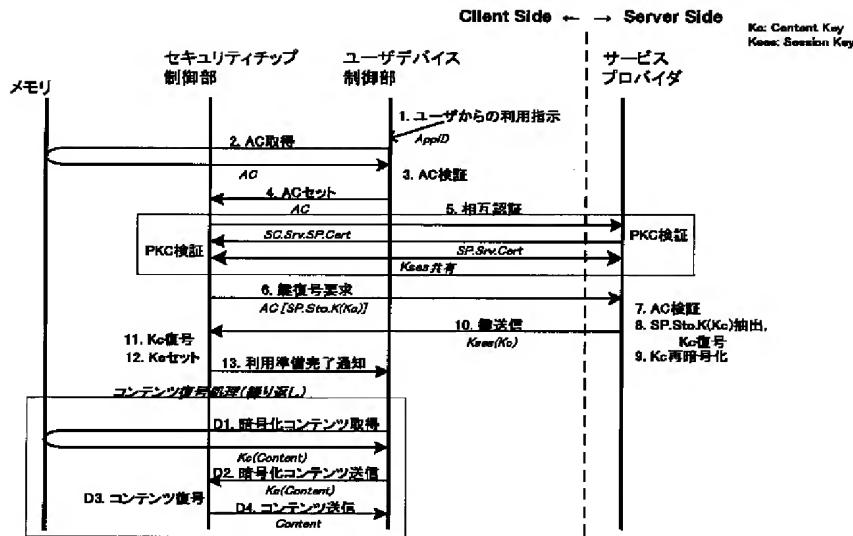
【図23】



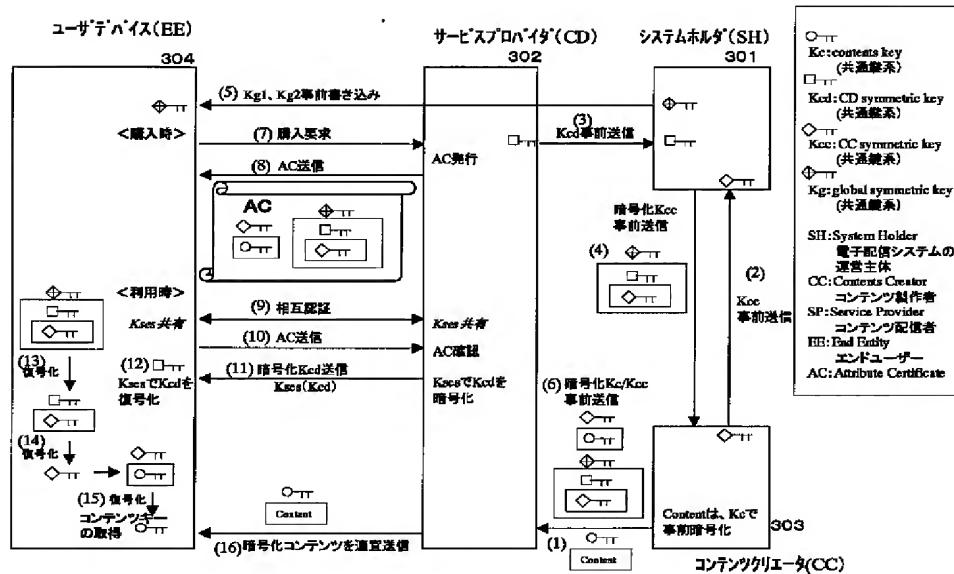
【図24】



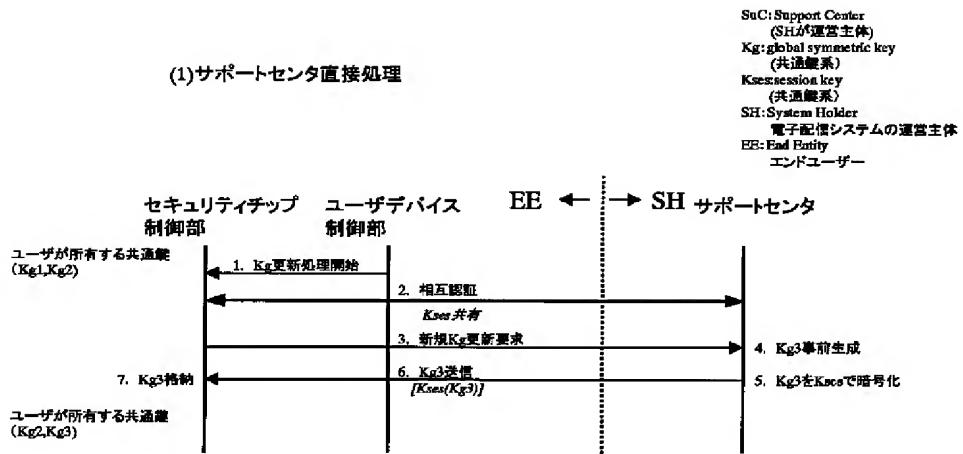
【図26】



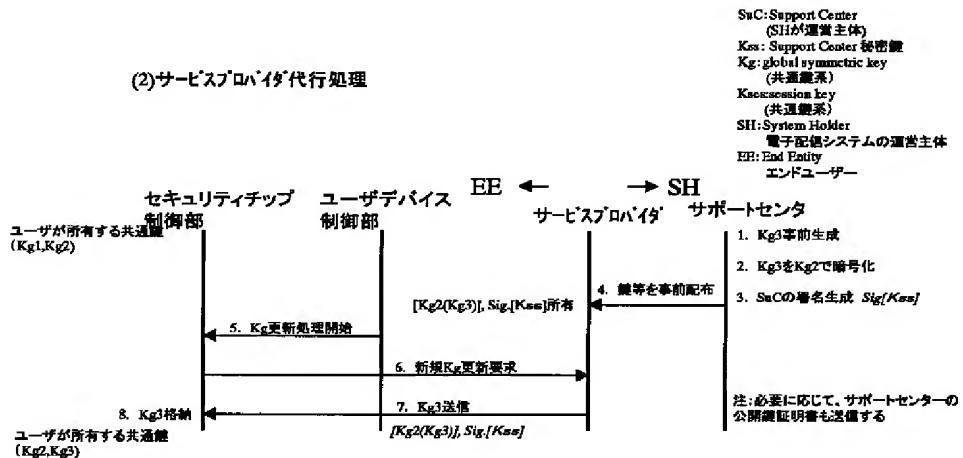
【図27】



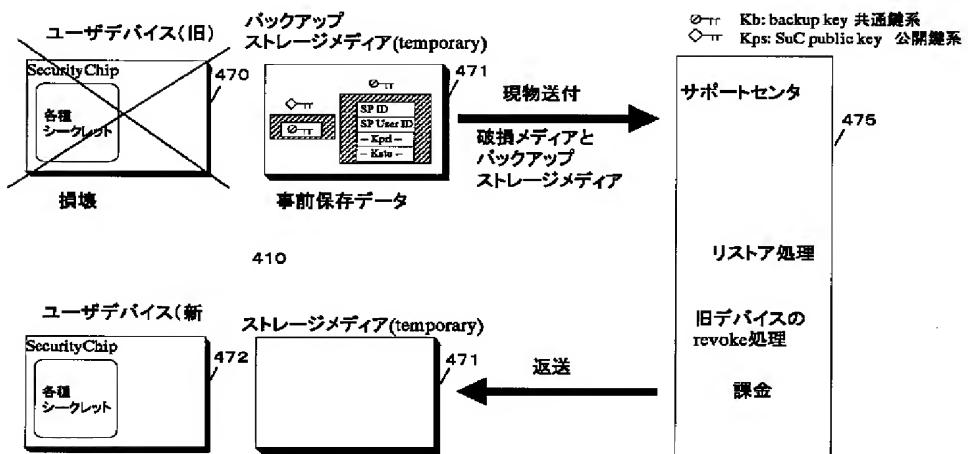
【図28】



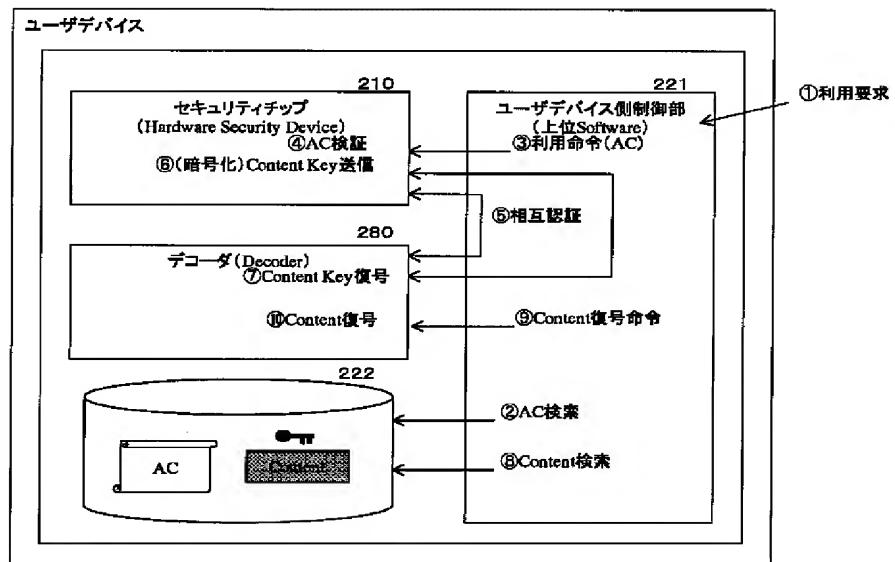
【図29】



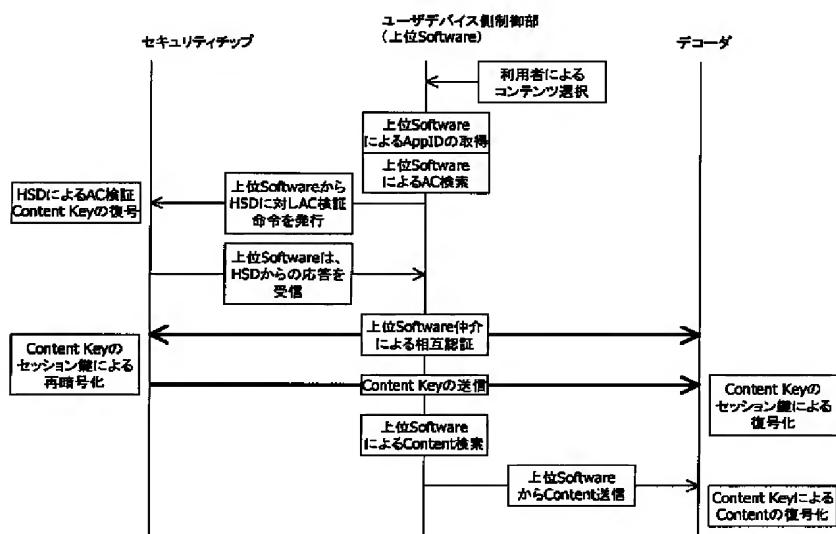
【図50】



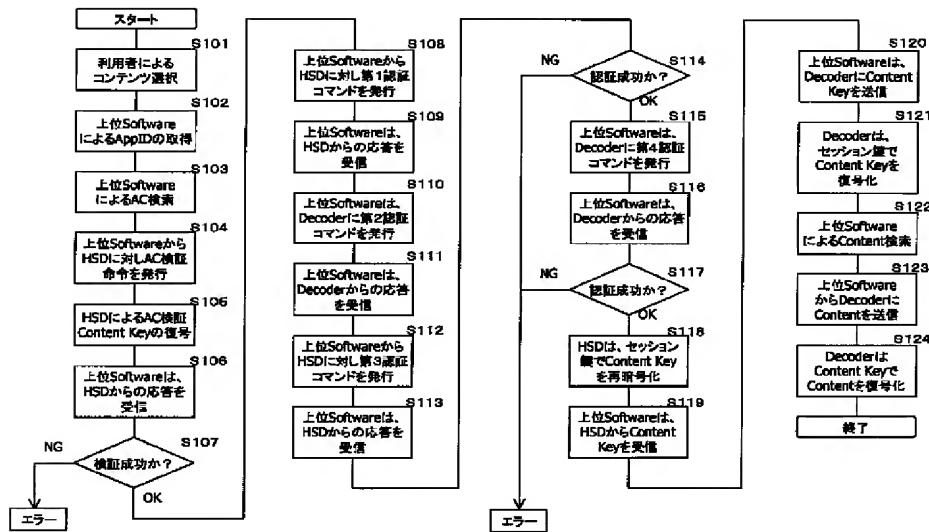
【図30】



【図31】

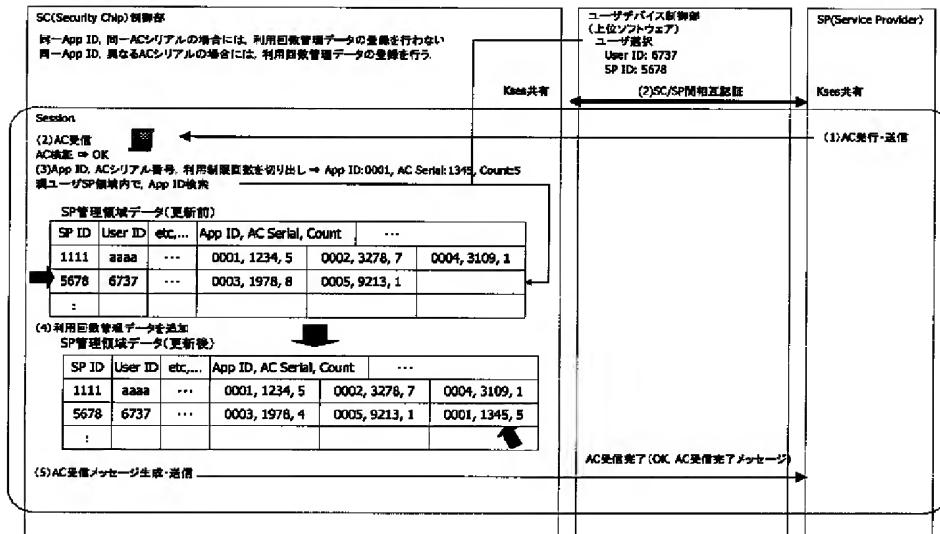


【図32】

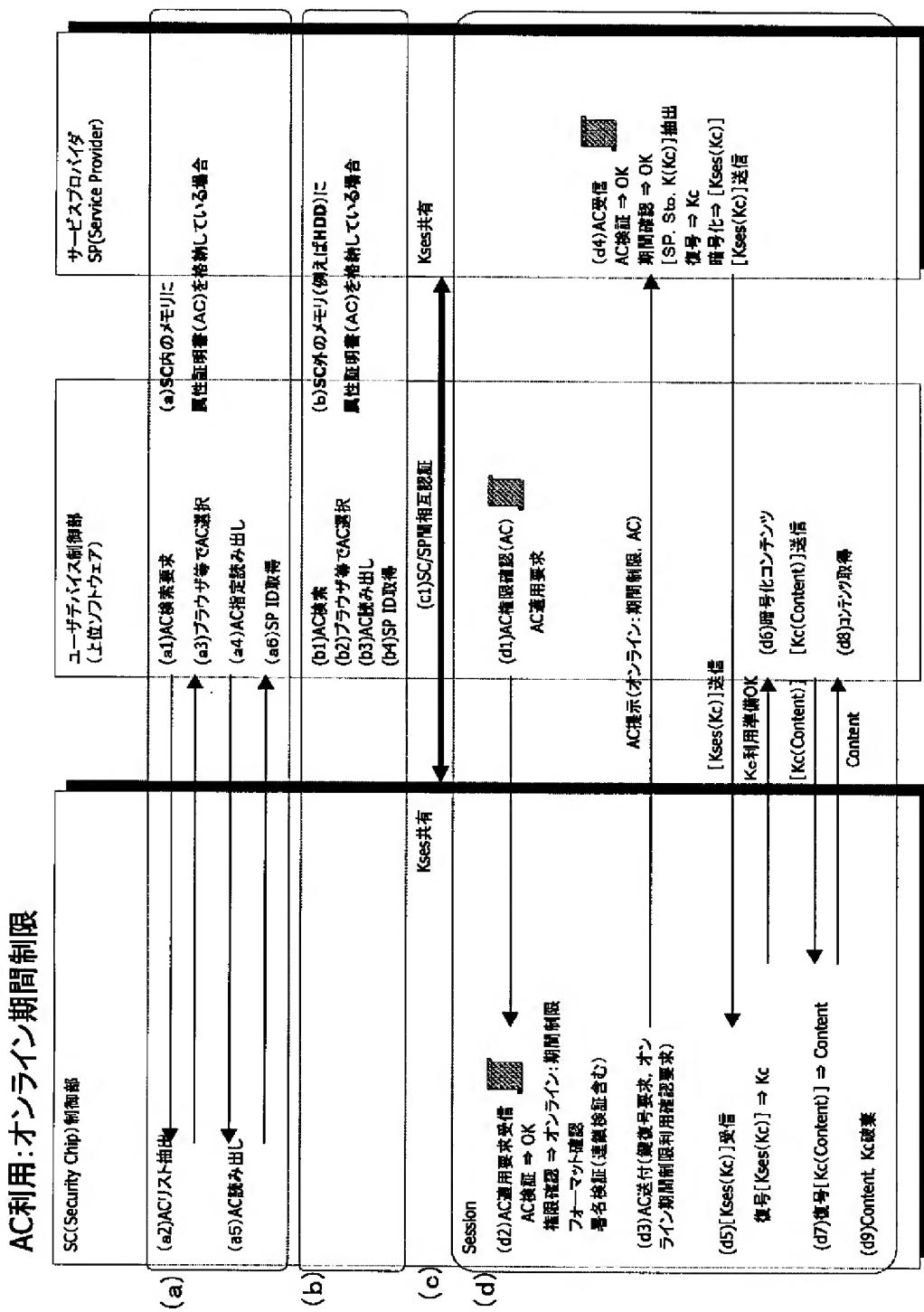


【図37】

## 利用回数管理データのインポート:回数管理

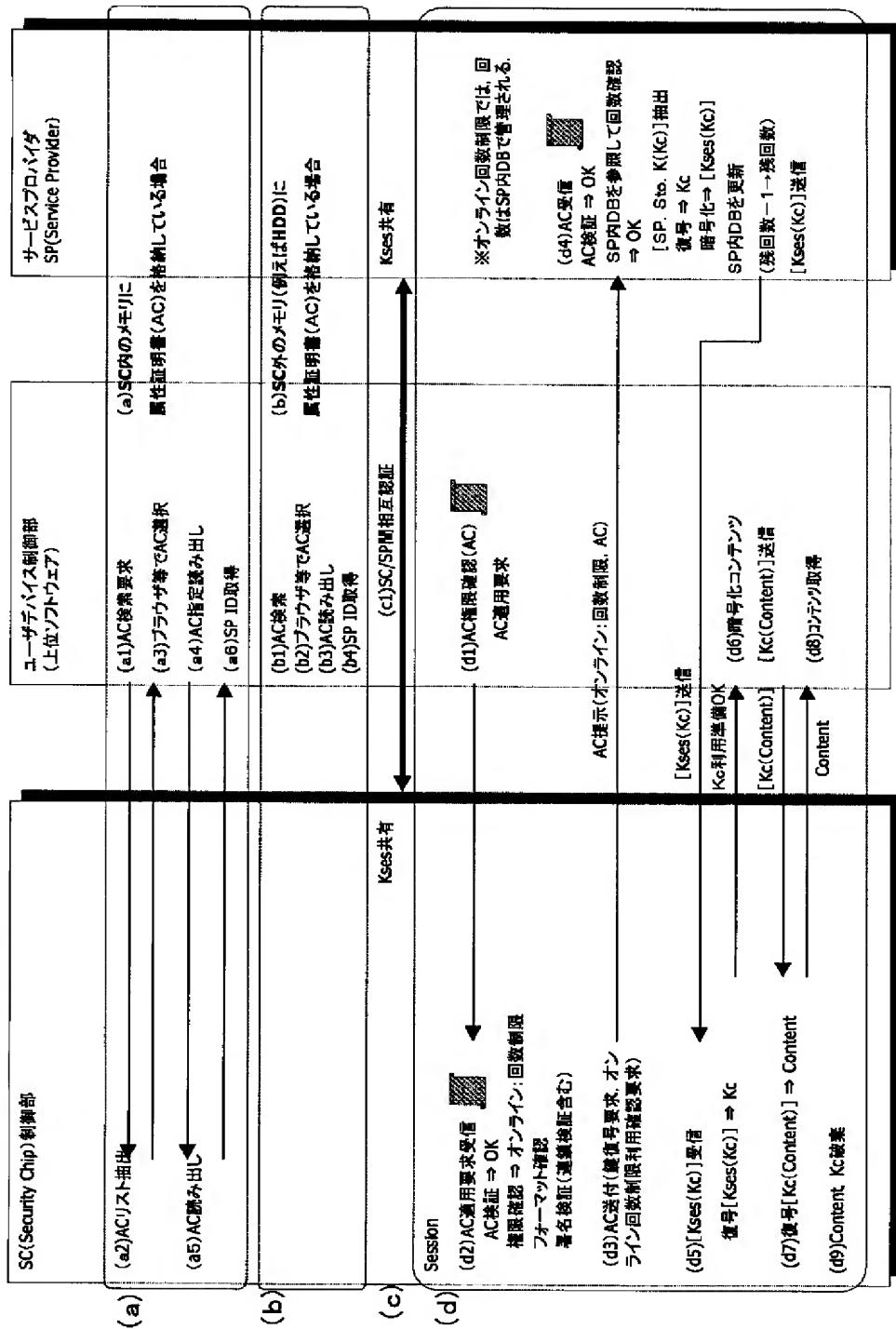


【図34】

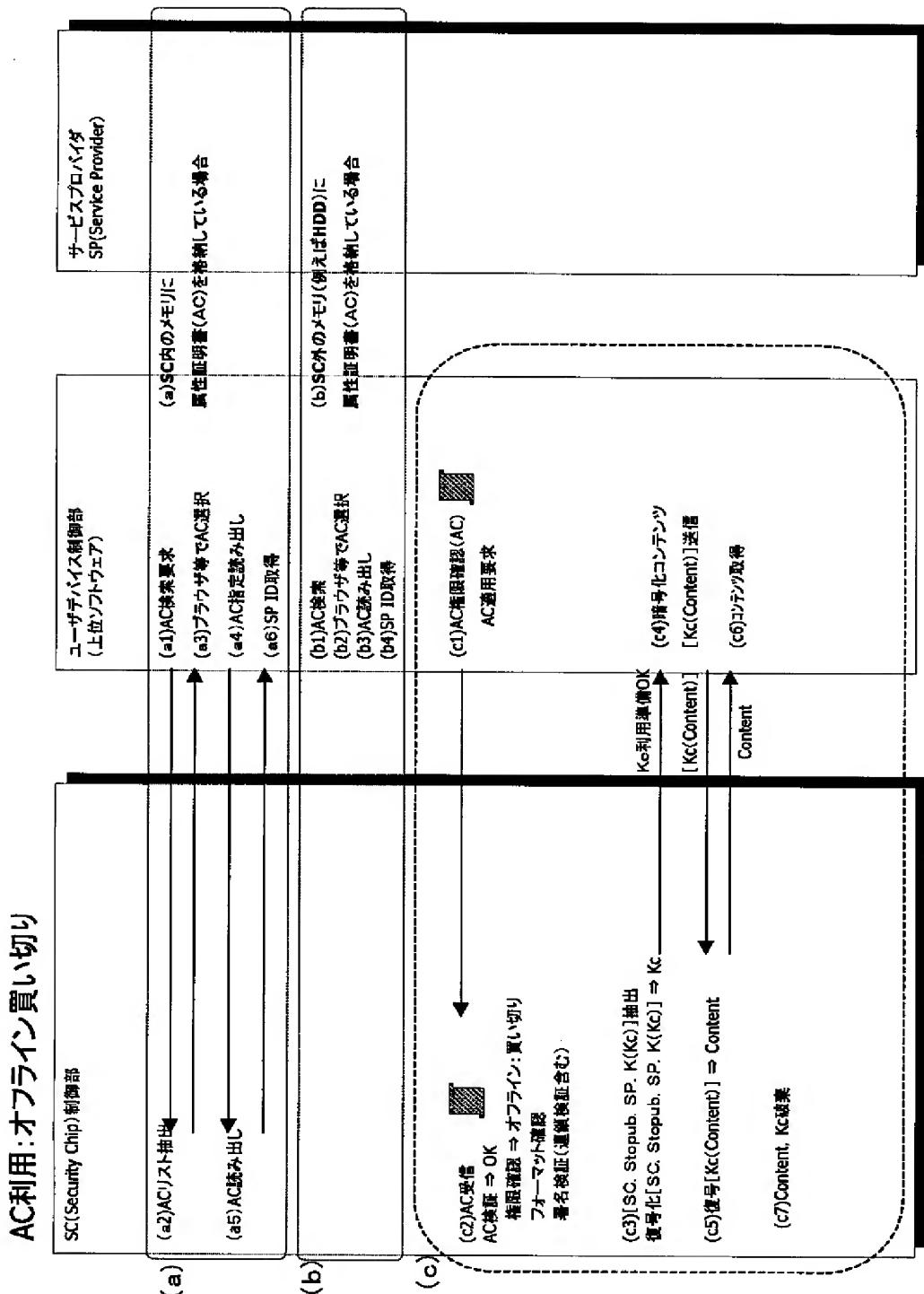


【図35】

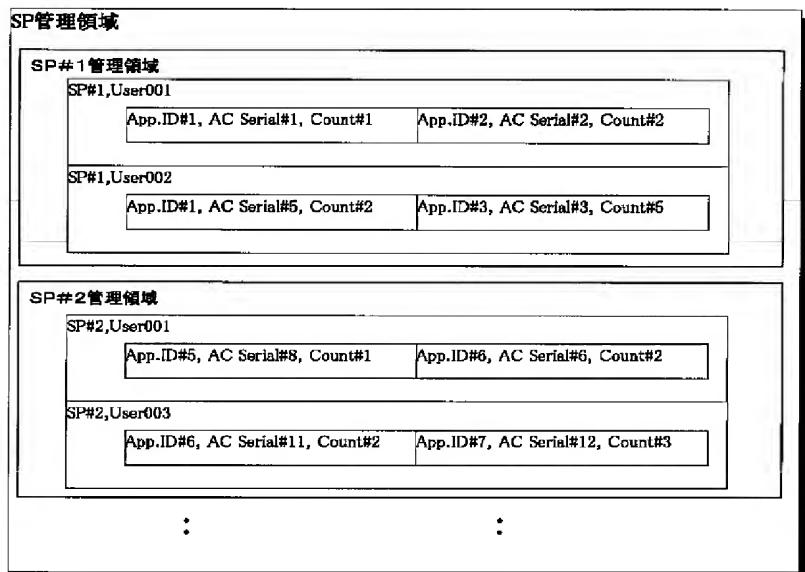
## AC利用:オンライン回数制限



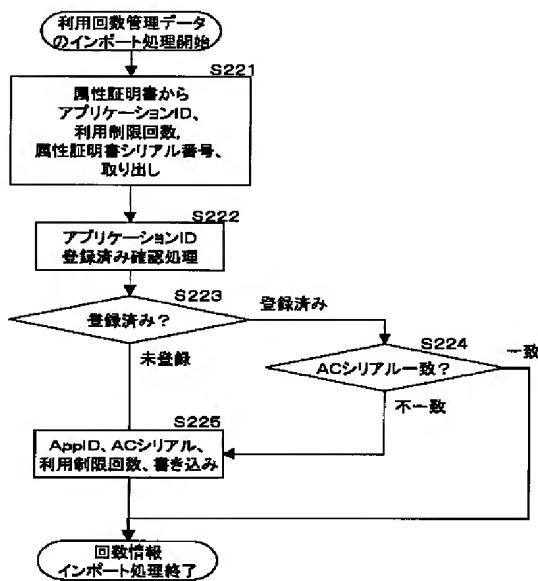
【図36】



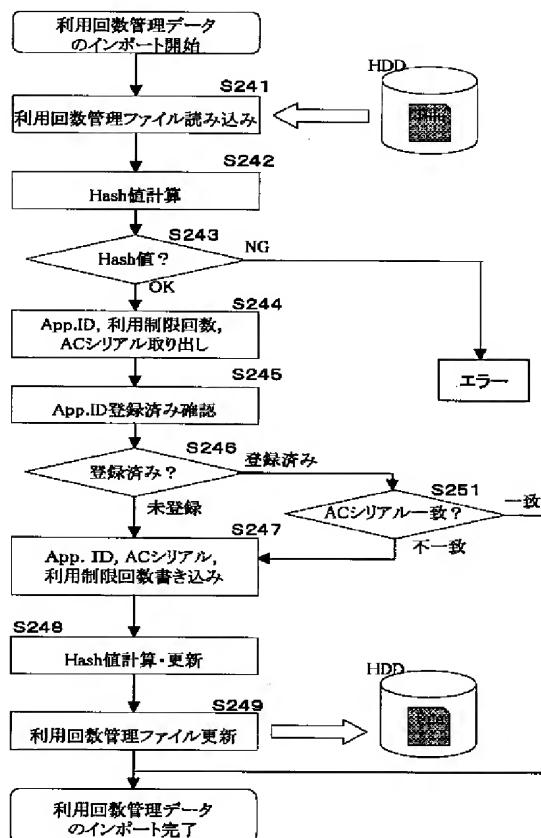
【図38】



【図39】

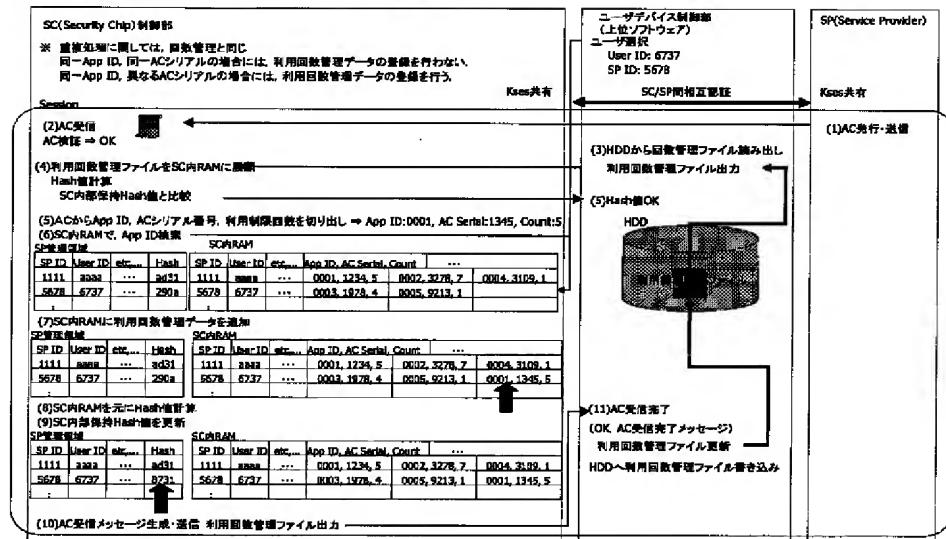


【図41】



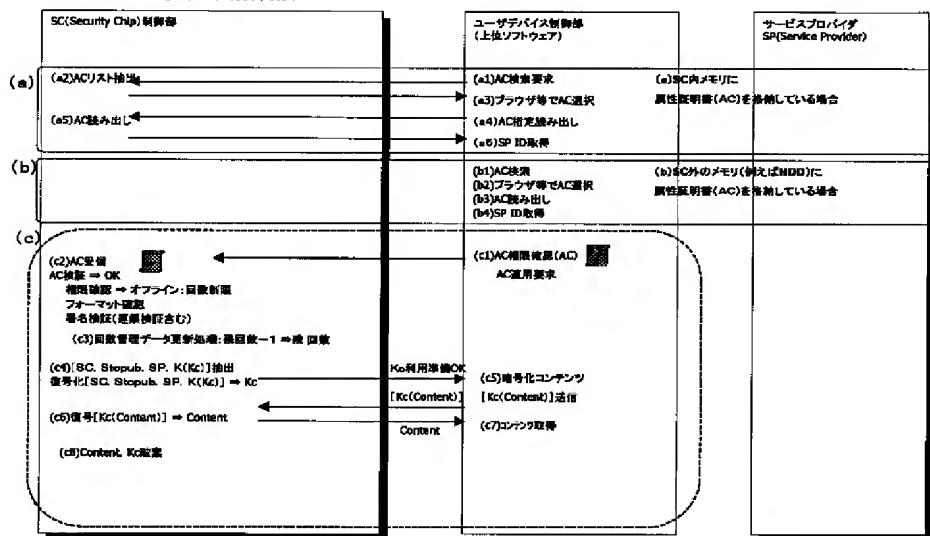
[図40]

## 利用回数管理データのインポート: Hash値管理



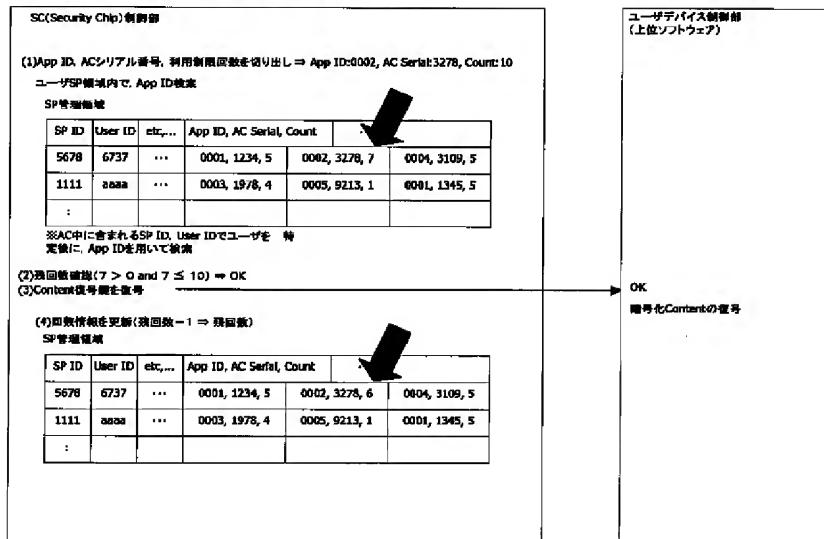
【図42】

AC利用:オフライン回数制限



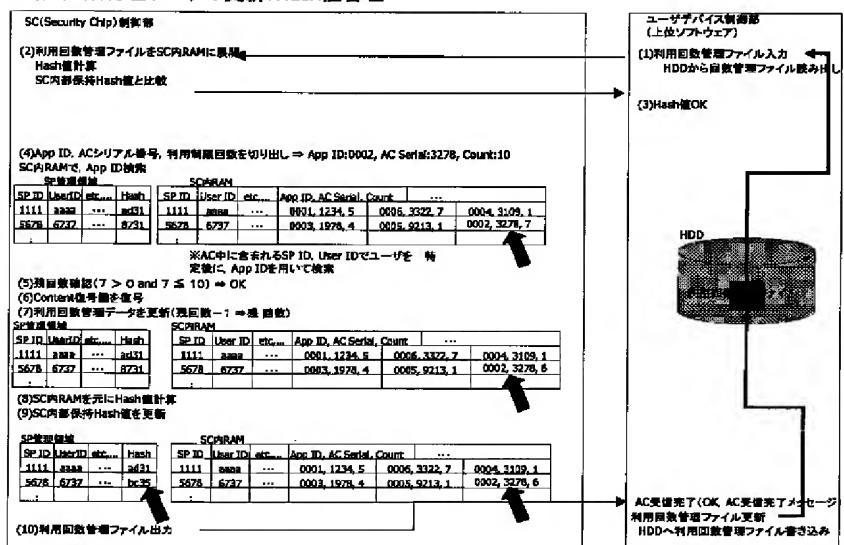
【図4.3】

## 利用回数管理データの更新: 回数管理



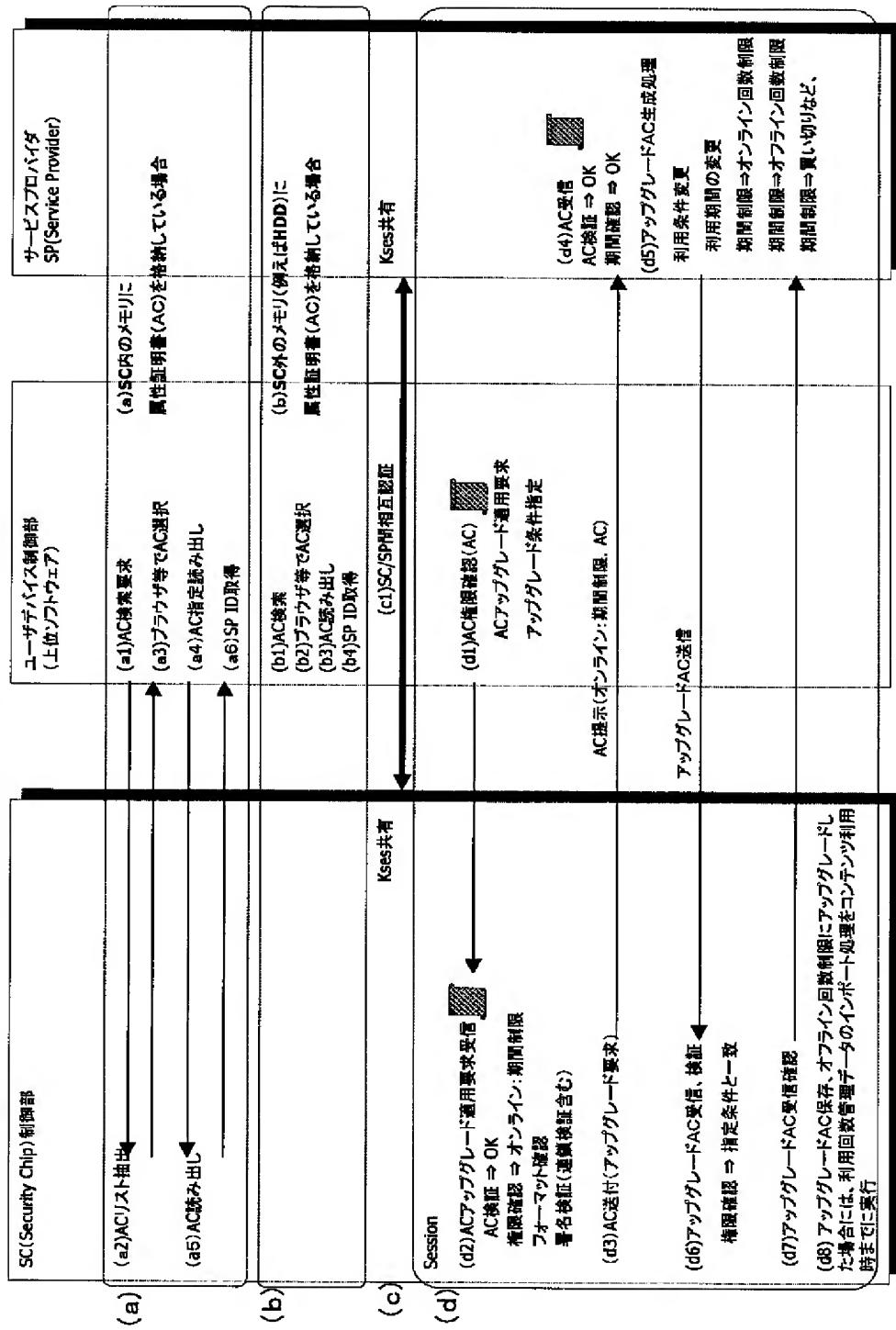
【図4.4】

## 利用回数管理データの更新: Hash値管理



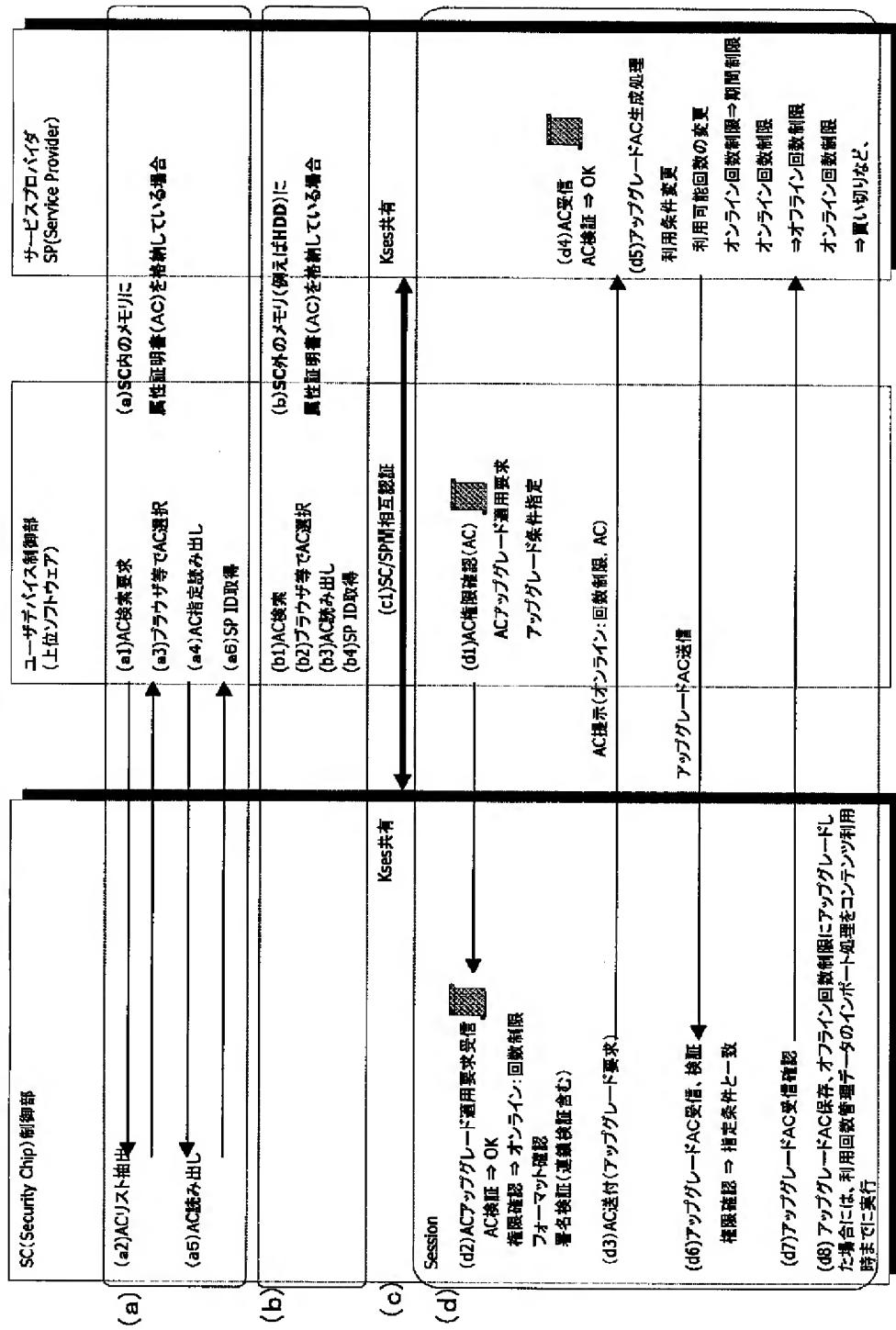
【図45】

## ACアップグレード:オンライン期間制限ACベース



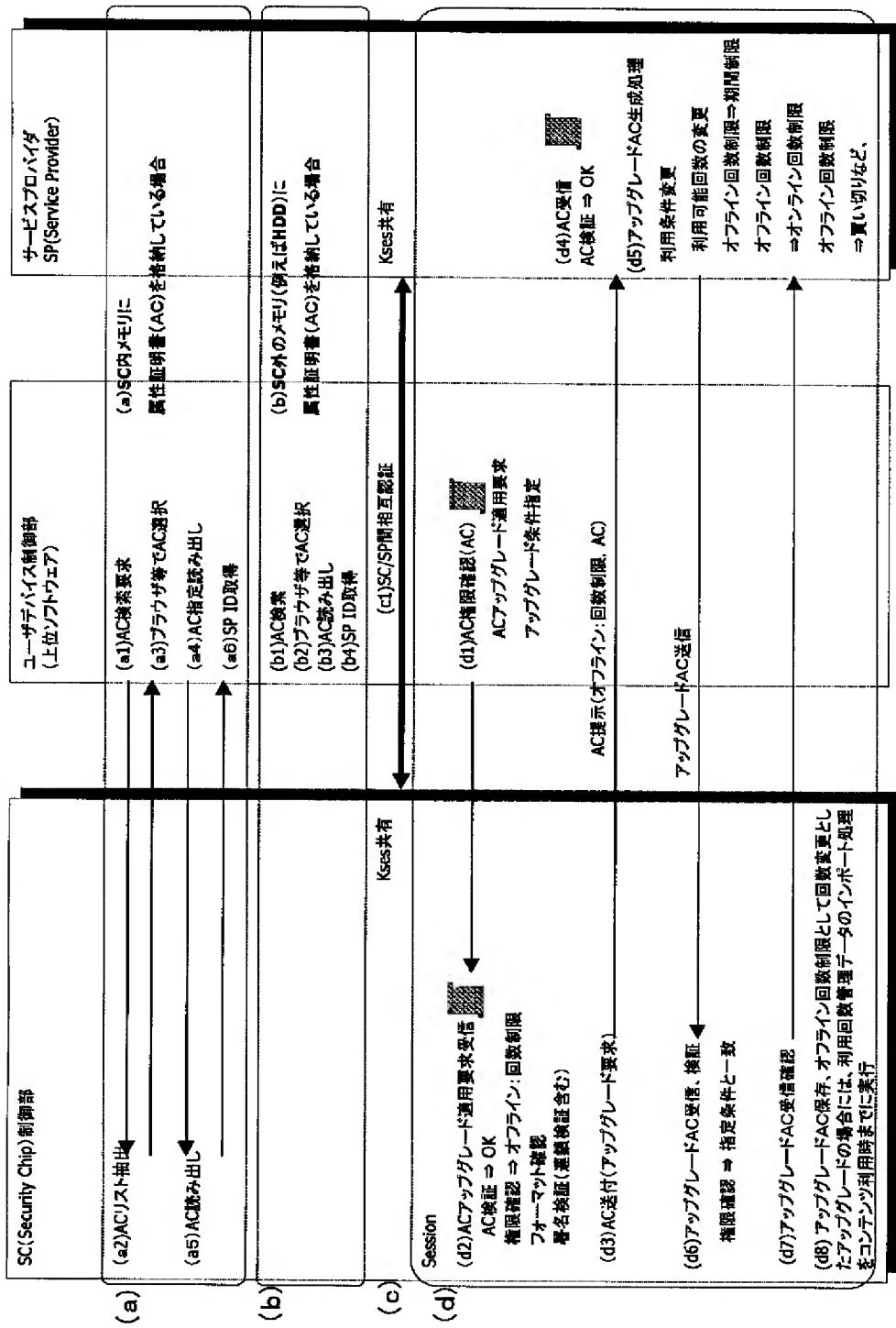
【図46】

## ACアップグレード:オンライン回数制限ACベース



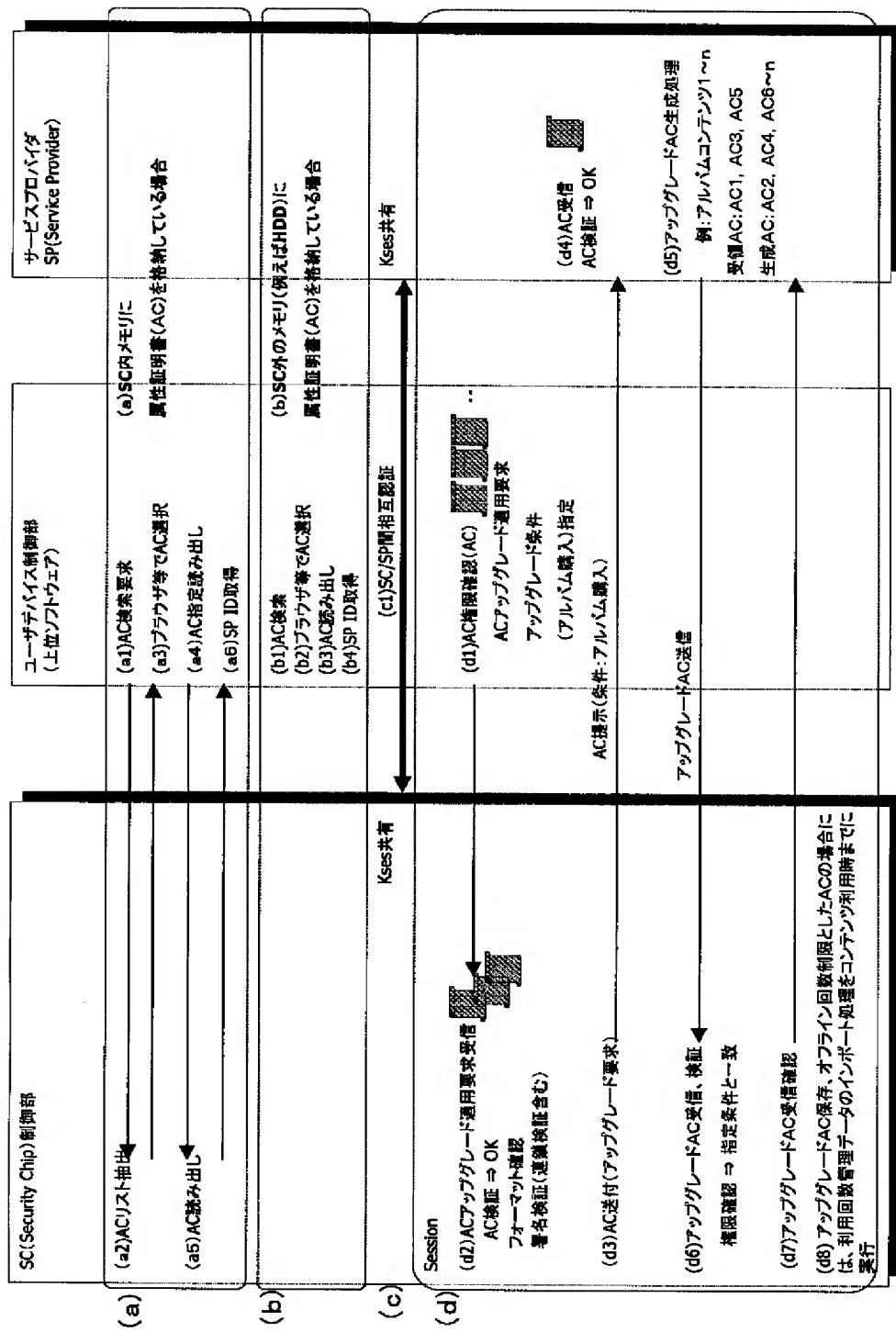
【図47】

## ACアップグレード:オンライン回数制限ACベース

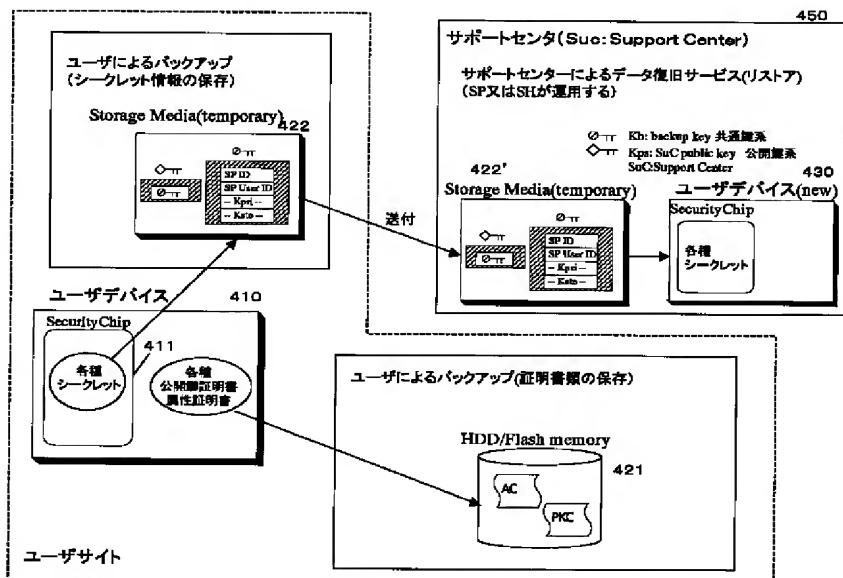


【図48】

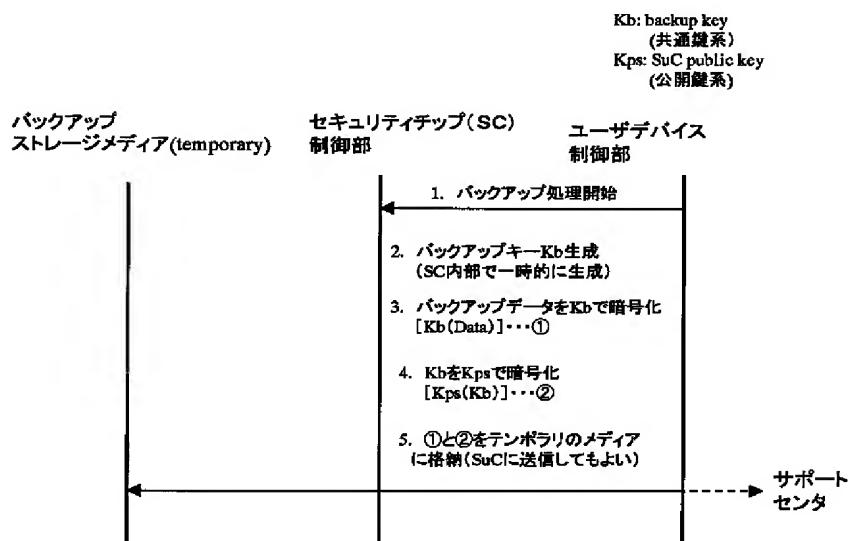
## ACアップグレード:アルバム購入



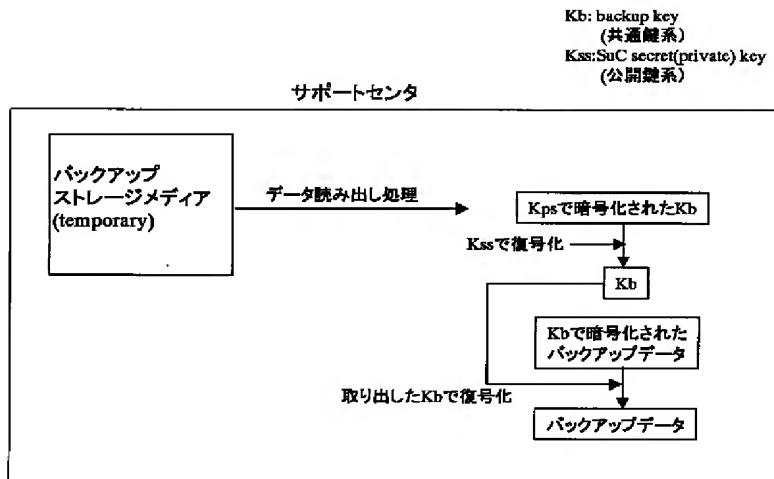
[図49]



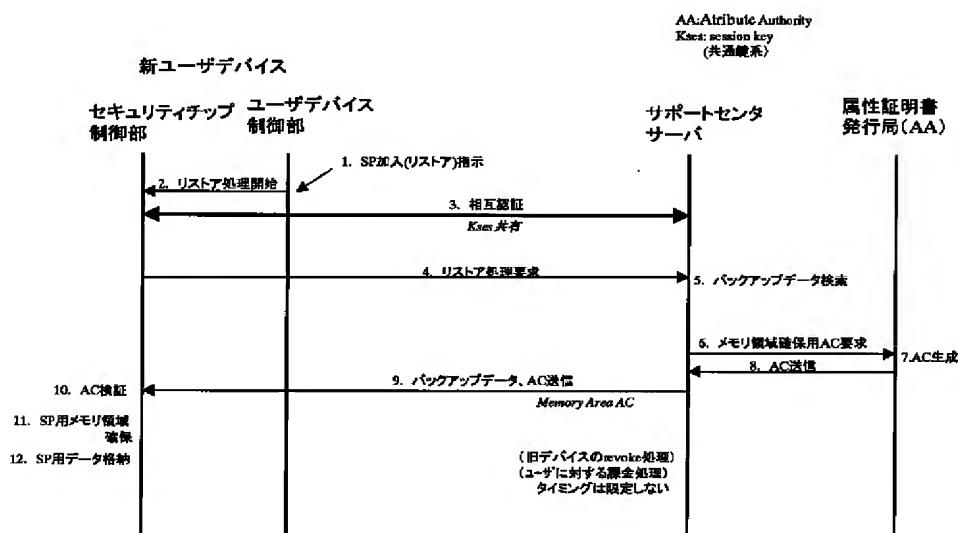
[図51]



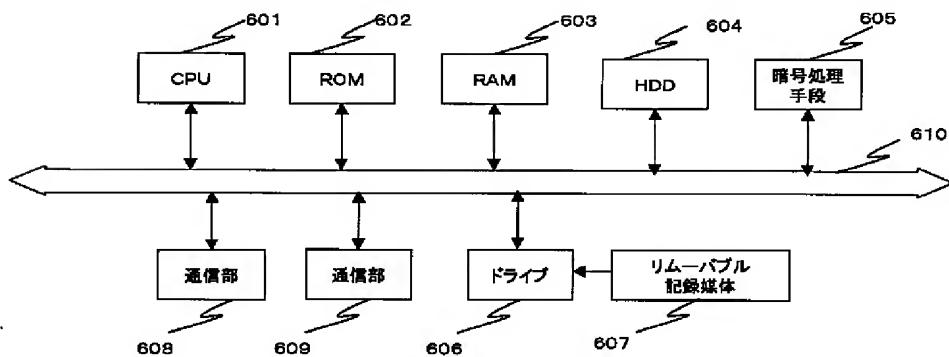
【図52】



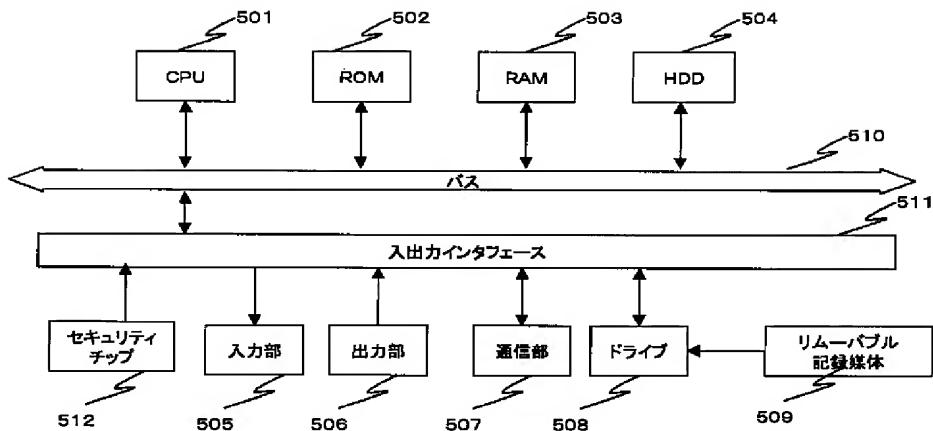
[図53]



[図55]



【図54】



フロントページの続き

(51)Int.Cl.<sup>7</sup>

識別記号

F I

テーマコード(参考)

H 04 L 9/32

H 04 L 9/00

6 0 1 E

6 7 5 B

(72)発明者 阿部 博

東京都品川区北品川6丁目7番35号 ソニ  
ー株式会社内

F ターム(参考) 5B017 AA03 BA07 CA16

5B018 GA04 HA05 KA22 MA12 NA06  
5B082 DE02

(72)発明者 岡 誠

東京都品川区北品川6丁目7番35号 ソニ  
ー株式会社内

5J104 AA07 AA16 EA05 EA06 EA19  
KA02 NA02 NA05 NA12 NA35  
NA36 NA37 NA42 PA07